International Journal of Security and Its Applications
Vol. 12, No. 1 (2018), pp.69-78
http://dx.doi.org/10.14257/ijsia.2018.12.1.06

A Qualitative Analysis of Information Privacy Concerns among Healthcare Employees

Fiza Abdul Rahim[1], Gopinath Muruti[2], Zuraini Ismail[3]
and Ganthan Narayana Samy[4]

[1,2]College of Computer Science and Information Technology, Universiti Tenaga Nasional
[3,4]Advanced Informatics School, Universiti Teknologi Malaysia
[1]fiza@uniten.edu.my, [2]gopinathmuruti@yahoo.com, [3]zues.ismail@gmail.com, [4]ganthan.kl@utm.my

Abstract

Healthcare organizations process massive amount of electronic medical records (EMR) utilized by their employees. Having given privileged access to sensitive and valuable patient information in the EMR, healthcare employees may cause privacy breaches, which may lead to detrimental consequences. Therefore, it is vital to impose particular attention to healthcare employees' concerns on privacy in the use of EMR. The purpose of this paper is to indicate the results from quantitative analysis (phase 1) through qualitative analysis (phase 2). From phase 1, privacy awareness is the only factor that influences information privacy concerns (IPC) in the use of EMR among healthcare employees, suggesting that healthcare employees do not think that privacy policy, privacy control, privacy risk, and privacy experience influence their IPC. To investigate why the respondents answered in this manner, the interviewees were asked to clarify why they think privacy awareness is very important to ensure the IPC among healthcare employees. Indeed, the mediating relationship of privacy awareness between privacy policy and IPC were discussed by highlighting on the implementation practices regarding privacy policy enforcement and awareness programs in healthcare organization.

Keywords*: Privacy Concerns, Electronic Medical Records, Qualitative*

1. Introduction

The massive growth of technology in the healthcare area have brought privacy issues and threats that have been emphasized by researchers and professionals [1–9]. There is a need for the data to be shared among healthcare employees and also third parties. For example, during an emergency situation, the data need to be shared with the rescuers for them to information about the patients and previous treatment history [10]. Patients are concerned about privacy threats and are worried if their personal information is being disclosed to other parties [11]. Patients elevated their concerns about organizational practices related to electronic medical records (EMR) collection and usage [11,12]. It is also suggested on the balance between the patient's desire for personal information protection against the need for information sharing among healthcare employees [14].

In Malaysia, the federal government has enforced the privacy protection act, Personal Data Protection Act (PDPA) starting on 15 November 2013. In exercise of the powers conferred by section 14 of the PDPA, a data user who belongs to any class of data users shall be registered under the Act. In line with the enacted act, organizations need to take specific measures related to privacy issues in ensuring their compliance to the act [15].

Received (August 16, 2017), Review Result (November 5, 2017), Accepted (November 24, 2017)

ISSN: 1738-9976 IJSIA

Because of these issues, this study attempts to indicate the results from quantitative analysis (phase 1) through qualitative analysis (phase 2) which discuss the factors that influence information privacy concerns (IPC). Although factors like privacy policy, privacy control, privacy risk and privacy awareness has been identified as influential factors of IPC in other privacy studies [16], only privacy awareness was found to be the only factor that influenced the IPC in quantitative analysis of this study, in addition privacy awareness was also found to have mediating effect towards privacy policy on IPC [17]. Therefore, a qualitative insight is needed to seek healthcare employees' explanations and provide possible clarification for the survey results. Their experiences and viewpoints may further assist in explaining the IPC among healthcare employees.

2. Related Works

In this study, the definition of information privacy concerns (IPC) is combines various terms used by Malhotra et.al [18], Park [19] and Tan et.al [20] which can be conceptually defined as employees' perception on privacy in the use of consumers' personal data being held by their organization. Although other researches related to IPC were carried out [20–23], limited attention was given to the aspect of employees' or users' perspective, who are the main members of the organization that handle patients' EMR.

Earp and Payton [22] reported that little number of researches have given extensive insight into the privacy practices of service industry workers, such as banking and healthcare employees who have access to personal data. In their study, they discovered that healthcare employees are highly concerned with errors in patient data whereas banking employees are more concerned about improper access of customer data.

Ball *et al*. [23] discovered that effective data protection trainings are associated with IPC. While Lebek and Breitner [24] found that employees' perceived uncertainty towards mobile devices usage due to security concerns, privacy concerns, and legal concerns. However, in this study, the determinants of IPC is examined comprehensively during the first stage [25], which expands the knowledge on what influences employees to be more concerned on the privacy of consumers' personal data.

Although few researches on IPC have been conducted in Malaysia [25–27], only one study were given attentions to the healthcare context [29]. Furthermore, all studies were only focused on consumers' perception. Hence, this motivates the need to know of factors that influence IPC among healthcare employees in Malaysia.

3. Methodology

The interviews were executed to evaluate and validate the findings from quantitative analysis. It was also aimed to uncover healthcare employees' perspective about IPC and the use of EMR in the healthcare organization. Interviewees were given Consent Form and Demographic Questionnaire before the interview session starts.

This study adopted a semi-structured interview where the interviews consisting of open-ended questions guided by questioning routes, listing of major topics and subsets of specific questions, as well as some other open-ended questions. The questioning routes were designed based on the method adopted by Patton [30] which starts by asking the interviewee about his/her background and demographic details.

Based on the last section in the questionnaire, the respondents were asked about their willingness to participate in the interview session. From the responses, the researcher contacts them using e-mail and telephone to confirm their participation in

the research. The date, time and location of the sessions that are convenient for the interviewees were decided during confirmation.

21 in-depth interviews were conducted among healthcare employees in the healthcare organization. Although the number of interviewees in the qualitative phase was smaller, this is not unusual in qualitative studies. This data not only explained the quantitative findings but added depth and richness to the data. Table 1 lists the details of the interviewees.

Table 1. Interviewees' Details

Employee Category	Respondent No.	Designation	Working Experiences (years)
Healthcare Professionals	HP1	Doctor	16
	HP2	Doctor	10
	HP3	Doctor	9
	HP4	Doctor	2
	HP5	Doctor	4
	HP6	Pharmacist	16
	HP7	Pharmacist	5
	HP8	Nurse	10
	HP9	Nurse	12
	HP10	Nurse	8
	HP11	Nurse	17
	HP12	Nurse	10
	HP13	Nurse	17
Healthcare Management Personnel	HM1	IT Officer	8
	HM2	IT Officer	11
	HM3	IT Officer	14
	HM4	IT Officer	10
	HM5	Medical Information Officer	15
	HM6	Medical Information Officer	12
	HM7	Administrative Officer	17
	HM8	Administrative Officer	5

For easy referencing of the agreed interviewees, the analysis on in-depth interviews is divided into two different groups: healthcare professionals and healthcare management personnel as presented in Table 1. There are 13 interviewees from the healthcare professionals group and 8 interviewees from healthcare management personnel group. Only four departments were involved from the healthcare professionals group: orthopedic, otorhinolaryngology, pharmacy, and nursing. Similarly, for the healthcare management personnel group, only four departments were involved: IT, health information, rehab, and ophthalmology.

The objectives of qualitative analysis are as follows:

(1) To investigate why healthcare employees think privacy awareness is important to ensure the IPC among healthcare employees.

(2) To obtain examples of the implementation practices regarding privacy policy enforcement and awareness programs in their healthcare organization.

Each interview session took around 20 to 30 minutes to complete. This study used convenience sampling, which focused on interviewees who volunteered to participate in this study. A follow-up recruitment letter was sent to all participants who agreed to participate in the interview session a week before the interview session was held. The letter contained the details about the interview session, venue, time, and the topic of discussion. A follow-up reminder via phone was also sent to the participants on the day before the interview session to remind them of it and to confirm their availability.

All interviewees were given an explanation about the research question, the definition of IPC and details on the identified factors that influence IPC to obtain more insight and in-depth responses. The interviews were only recorded if permission is received from the interviewees and notes were taken where necessary.

The interviews were mostly conducted in English. However, some of the interviewees were more comfortable to be interviewed bilingually. Then, both Malay and English or in Malay only were used throughout the interview depending on the interviewees' preferences.

The process of data analysis starts with data preparation, which involves interview transcribing to word processor text. The interview transcripts were organized into designated files for easy retrieval. The transcribed interviews were coded into qualitative data analysis software, ATLAS.ti. The coding process was performed to analyze the transcribed interviews. The final step is concluded when similar emerging themes are categorized together.

3. Findings

The findings from the qualitative analysis are presented as a series of themes organized under the following key topics:

(1) The significant finding of privacy awareness as an influential factor of IPC; and

(2) Implementation practices regarding privacy policy enforcement and awareness programs.

3.1. Privacy Awareness as an Influential Factor of IPC

To help understand the importance of privacy awareness among healthcare employees, interviewees were asked to explain how privacy awareness influences IPC. Based on their responses, two areas have been identified that connect the privacy awareness among healthcare employees to their concern in the use of EMR: 1) The importance of privacy awareness in healthcare field; and 2) Responsibility on creating privacy awareness among healthcare employees.

3.1.1. The Importance of Privacy Awareness in Healthcare Field

Three interviewees indicated at some point during the interview that privacy awareness is important in healthcare field. From the healthcare professionals group, they strongly voiced out their concerns on privacy awareness among healthcare employees. The following are comments made by the three healthcare professionals on the issue of privacy awareness:

"Privacy is a must and the employer should inform the staff about what they must follow, PDPA for example..."

[HP2, Doctor]

"…the most important thing in privacy is that the information must not get into the wrong hands.

[HP6, Pharmacist]

"I know about privacy when it relates with consent. For example, in my ward, hospital must get consent from parents before performing any procedures on their children. In

cases of emergency, usually I am the one who will contact the parents when they are not around their children to inform about the treatment suggested by the doctors."

[HP11, Nurse]

The healthcare professionals believed that informing the importance of privacy in the use of EMR has a lot to do with the present concerns and actions of the healthcare employees and that finding showed a crucial aspect in IPC. This is clearly demonstrated through the steps that must be followed in every procedure to ensure the privacy of EMR is preserved.

3.1.2. Responsibility on Creating Privacy Awareness among Healthcare Employees

From healthcare management personnel's viewpoints, there is a disagreement in terms of responsibility creating privacy awareness among healthcare employees. In current situation, IT department is currently responsible sending e-mail to alert users on spamming and virus. They also regularly update users on any new security threats to mitigate the possibility of downloading malicious files, engaging with affected files by using flash drives, which may cause the computer to function improperly. Some of arguments made by three interviewees commenting on the responsibility to create privacy awareness among healthcare employees:

"...IT department is not responsible in creating awareness on privacy, we are responsible in providing support."

[HM1, IT Officer]

"I think the head of department of IT should take the responsibility towards creating awareness about privacy, but it seems that no specific unit is there specifically takes care of privacy and security."

[HM4, IT Officer]

"...Every single perspective should be clarified before the full implementation of EMR. IT department, Health Information Department, doctors, nurses, and the top management must decide who is responsible on the effort to create awareness. But, from my personal opinion, it should be under the responsibility of every head of departments to ensure that their staffs are aware on the responsibility to protect the privacy of EMR. It is clearly stated in the PDPA, top management is mainly responsible, followed by all head of departments."

[HM6, Medical Information Officer]

Indeed, there is a need for training and exposure to increase healthcare employees' understanding on privacy. However, majority of the respondents mentioned that IT department only conduct several training series when introducing users to new modules created in the system. Moreover, according to five doctors (HP1, HP3, HP4, HP5, and HP6), there was no security training conducted that clearly highlights the importance of privacy. Therefore, it is difficult to ensure that an employee has enough information about the privacy of EMR. HP1 advocated based on his comment:

"I think I have received only one pamphlet about security but it was more than 5 years ago. Someone or a specific department should take the responsibility to let user know what they should do, and what needs to be avoided. However, I do always remind my staffs, do not share any information about patients through social media. It is a trend nowadays right, selfie with patients. For me, it is unethical. That is why I do always highlight this issue from time to time."

[HP1, Doctor]

The current implementation of training processes focused on how to use the EMR, whereas interviewees feel that the importance of privacy and security values should be integrated into the current training module. All interviewees from the healthcare professionals group noticeably mentioned that there is no security or privacy training being held since the first day they started working. The following quotes reflect concerns among healthcare professionals regarding privacy training:

"I never attended any security or privacy trainings, and I don't think there is any security or privacy training ever being held in this hospital."
[HP1, Doctor]
"…there is no such formal training being given with regards to privacy."
[HP6, Pharmacist]

"Since we are about to launch another new module next year, our planning is to embed security and privacy issues in the training."
[HM2, IT Officer]

Without proper training and introduction to the privacy requirements that needs to be complied by the healthcare employees, it may be perceived as an additional workload for the healthcare employees if they need to explore about the requirements on their own. A specific department should be appointed to manage and design how privacy requirements can be successfully delivered to all healthcare employees.

Interviewee HP9 highlighted the importance of privacy awareness through her apprehension in password compromise. Based on her statement about frequently changing her password once she doubts that her password was compromised, it shows that privacy awareness makes her think on what needs to be done in order to protect her accessibility, which contains EMR in the system.

"When I feel that my password is known by others, I will immediately change my password. I do not want others to see the confidential information inside the system, and specifically I do not want others creating a mess by using my username in doing any possible illegal activity."
[HP9, Nurse]

The support from IT department is also crucial especially in ensuring that technical support is well delivered. Here is one criticism made by an IT officer cum database administrator (HM4), which highlights on the fact that countermeasures only are taken after privacy breach events have already occurred.

"I am only in-charge of the database but no specific task was given to me about protecting privacy of EMR. As what users can see in the system, the same information also will be seen in the database since there are no additional features to protect privacy and security. From my personal opinion, top management did not emphasise about security until the huge case happened. This is not the correct way. I have a lot of suggestions to protect privacy of EMR but they are never interested to listen before this."
[HM4, IT Officer]

These two themes showed that healthcare employees require awareness as a vehicle for helping them in raising their concerns on the privacy of EMR. Despite a number of privacy awareness issues, especially in terms of responsibilities, there is no doubt that the significant influential factor of IPC is due to the healthcare employees' awareness on the importance of privacy in the use of EMR. The interviewees also agreed that IPC in the use of EMR is unlikely if the healthcare employees' awareness is left out at the initial point.

3.2. Implementation Practices Regarding Privacy Policy Enforcement and Awareness Programs

Quantitative analysis in phase 1 of this study concluded that privacy awareness has indirect-only mediation of the relationship between privacy policy and IPC. To help understand the importance of privacy awareness as a mediator between privacy policy and IPC, interviewees were asked to describe what are the implementation practices regarding privacy policy enforcement and awareness programs in their healthcare organisation.

One of the medical information officers also emphasised on the relationship between privacy awareness and privacy policy. Based on her understanding, privacy awareness and privacy policy are interrelated:

"Awareness starts if the top management gives a clear instruction and direction to explain to all staffs that our hospital is subjected to PDPA and they must bear with the requirements. Although, the privacy policy must be outlined from various perspectives, which includes doctors, nurses, IT department, health information department and other related departments to ensure the smooth process when it comes to creating the awareness later on."

[HM6, Medical Information Officer]

In the process of the full implementation of EMR which later involves handling massive data, healthcare organisations must also consider a proper guideline constructed by gathering input from the government, other healthcare providers, or patients' opinion. The development of privacy guidelines must also be tailored to needs of the healthcare settings. The following are comments from healthcare professionals on privacy guidelines, which are obviously not being stressed enough by the top management:

"If we are required to abide by the PDPA, then a clear privacy guidelines must be designed which is tailored to our needs in the healthcare settings."

[HP6, Pharmacist]

"This organisation should have a clear procedure especially to entertain new users. They should be briefed on what should be done and what is restricted in the use of EMR."

[HP11, Nurse]

"There is no strict procedure to reset password, the authentication is only staff identification number. It is suggested to get approval from head of department before any request is submitted to the IT department."

[HP12, Nurse]

"I don't think we have an exit policy in this hospital which any employees who are no longer working in this hospital, automatically their credentials will be no longer be used and expires automatically. The funny situation happened here, some of doctors are still using username and password owned by previous doctor who are no longer working for this hospital. This situation should not have happened."

[HP3, Doctor]

Similar viewpoints are also given by the following quotes from healthcare management personnel:

"As far as I concern, there are no privacy guidelines in this hospital. But we are preparing to discuss further on this issue during the security policy review next month."

[HM1, IT Officer]

"The Act should be referred to as the main reference in drafting customised privacy guidelines for this hospital."

[HM2, IT Officer]

In the development process of privacy guidelines, legislation is one of the most important key elements to be emphasised and embedded in the guidelines. As PDPA enlisted the general guidelines in securing privacy, healthcare organisation must itemise the contents to be tailored with the healthcare settings.

4. Conclusion

The results from follow-up interviews in this study could assist the healthcare organizations, in their employees' IPC. It is highly recommended that healthcare organization take into account the influential factors of IPC in the use of EMR among their healthcare employees.

At the organization level, healthcare organization may implement awareness program to promote the understanding and implementation of privacy policy for their healthcare employees. At the national level, Ministry of Health (MOH), may conduct more awareness campaigns on privacy to promote the understanding and

implementation of privacy control mechanisms in protecting EMR. Likewise, awareness initiatives by the Personal Data Protection Department, under the Ministry of Communication and Multimedia, should always be in the headlines to enhance privacy awareness among public. These initiatives are important to ensure the compliance with the PDPA.

References

[1] R. F. Parks, C.-H. Chu, H. Xu and L. Adams, "Understanding the Drivers and Outcomes of Healthcare Organizational Privacy Responses", in Thirty Second International Conference on Information Systems, no. 2, **(2011)**, pp. 1–20.
[2] G. N. Samy, R. Ahmad and Z. Ismail, "Threats to Health Information Security", in 2009 Fifth International Conference on Information Assurance and Security, **(2009)**, pp. 540–543.
[3] A. Appari and M. E. Johnson, "Information security and privacy in healthcare: current state of research", Int. J. Internet Enterp. Manag., vol. 6, no. 4, **(2010)**, pp. 279–314.
[4] P. Ambrose and C. Basu, "Interpreting the Impact of Perceived Privacy and Security Concerns in Patients' Use of Online Health Information Systems", J. Inf. Priv. Secur., vol. 8, no. February 2015, **(2015)**, pp. 38–50.
[5] D. Birnbaum, E. Borycki, B. T. Karras, E. Denham and P. Lacroix, "Addressing Public Health informatics patient privacy concerns", Clin. Gov. An Int. J., vol. 20, no. 2, **(2015)**, pp. 91–100.
[6] W. Chung and L. Hershey, "Enhancing Information Privacy and Data Sharing in a Healthcare IT Firm: The Case of Ricerro Communications", J. Inf. Priv. Secur., vol. 8, no. February 2015, **(2014)**, pp. 56–78.
[7] T. Ermakova, B. Fabian, and R. Zarnekow, "Security and Privacy System Requirements for Adopting Cloud Computing in Healthcare Data Sharing Scenarios", in Proceedings of the Nineteenth Americas Conference on Information Systems, **(2013)**, pp. 1–9.
[8] I. C. S. José Luis Fernández-Alemán, P. Á .O. Lozoya and A. Toval, "Security and privacy in electronic health records: A systematic literature review", J. Biomed. Inform. , **(2013)**, pp. 1–22.
[9] I. Carrión Señor, J. L. Fernández-Alemán and A. Toval, "Are personal health records safe? A review of free web-accessible personal health record privacy policies", J. Med. Internet Res., vol. 14, no. 4, **(2012)**, p. e114.
[10] A. A. Bakar, A. A. Ghapar and R. Ismail, "Access control and privacy in MANET emergency environment", in 2014 International Conference on Computer and Information Sciences (ICCOINS), **(2014)**, pp. 1–6.
[11] J. Kolter and G. Pernul, "Generating User-Understandable Privacy Preferences", in 2009 International Conference on Availability, Reliability and Security, **(2009)**, pp. 299–306.
[12] H. J. Smith, T. Dinev and H. Xu, "Information Privacy Research: An Interdisciplinary Review", MIS Q., vol. 35, no. 4, **(2011)**, pp. 989–1015.
[13] H. J. Smith, S. J. Milberg and S. J. Burke, "Information Privacy: Measuring Individuals' Concerns About Organizational Practices", MIS Q., vol. 20, no. 2, **(1996)**, pp. 167–196.
[14] Y. Niimi and K. Ota, "Examination of an Electronic Patient Record Display Method to Protect Patient Information Privacy", CIN Comput. Informatics, Nurs., vol. 35, no. 2, **(2017)**.
[15] S. Zulhuda and A. Ibrahim, "The State of E-Government Security in Malaysia : Reassessing the Legal and Regulatory Framework on the Threat of Information Theft", in ICCIT 2012, **(2012)**, pp. 810–815.
[16] L. N. Zlatolas, T. Welzer, M. Heričko and M. Hölbl, "Privacy antecedents for SNS self-disclosure: The case of Facebook", Comput. Human Behav., vol. 45, **(2015)**, pp. 158–167.
[17] F. Abdul Rahim, Z. Ismail and G. Narayana Samy, "Healthcare employees' perception on information privacy concerns", in 2017 International Conference on Research and Innovation in Information Systems (ICRIIS), **(2017)**, pp. 1–6.
[18] N. K. Malhotra, S. S. Kim and J. Agarwal, "Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model", Inf. Syst. Res., vol. 15, no. 4, **(2004)**, pp. 336–355.
[19] I. Park, "The Study on The Relationship Between Privacy Concerns and Information Systems Effectiveness", in International Conference on Information Systems (ICIS), **(2009)**.
[20] X. Tan, L. Qin, Y. Kim and J. Hsu, "Impact of privacy concern in social networking web sites", Internet Res., vol. 22, no. 2, **(2012)**, pp. 211–233.
[21] J. B. Earp and F. C. Payton, "Data Protection in the University Setting : Employee Perceptions of Student Privacy", in Proceedings of the 34th Hawaii International Conference on System Sciences - 2001, vol. 0, no. c, **(2001)**, pp. 1–6.
[22] J. B. Earp and F. C. Payton, "Information Privacy in the Service Sector: An Exploratory Study of Health Care and Banking Professionals", J. Organ. Comput. Electron. Commer., vol. 16, no. 2, **(2006)**, pp. 105–122.
[23] K. Ball, E. M. Daniel and C. Stride, "Dimensions of employee privacy: an empirical study", Inf. Technol. People, vol. 25, no. 4, **(2012)**, pp. 376–394**.**
[24] B. Lebek and M. H. Breitner, "Investigating the Influence of Security, Privacy, and Legal Concerns on Employees â€™ Intention to Use BYOD Mobile Devices", no. 2008, **(2013)**, pp. 1–8.

[25] F. A. Rahim, Z. Ismail and G. N. Samy, “Healthcare employees’ perception on information privacy concerns”, 2017 Int. Conf. Res. Innov. Inf. Syst., no. November 2013, **(2017)**, pp. 1–6.
[26] N. Mohamed and I. H. Ahmad, “Privacy Measures Awareness , Privacy Setting Use and Information Privacy Concern with Social Networking Sites”, in International Conference on Research and Innovation in Information Systems (ICRIIS), 2011, no. November, **(2011)**.
[27] M. Lallmahamood, “An Examination of Individual ’ s Perceived Security and Privacy of the Internet in Malaysia and the Influence of This on Their Intention to Use E-Commerce : Using An Extension of the Technology Acceptance Model”, J. Internet Bank. Commer., vol. 12, no. 3, **(2007)**, pp. 1–26.
[28] M. Lallmahamood, “Privacy over the Internet in Malaysia : A Survey of General Concerns and Preferences among Private Individuals”, Malaysian Manag. Rev., vol. 43, no. 1, **(2008)**, pp. 77–108.
[29] S. Samsuri and Z. Ismail, “Personal Medical Information Management : The Information Privacy Culture of Asian Countries”, J. Econ. Bus. Manag., vol. 1, no. 4, **(2013)**, pp. 329–333.
[30] M. Q. Patton, "Qualitative research and evaluation methods", 3rd Editio. Thousand Oaks, CA: SAGE Publications, Inc, **(2002)**.

