

# Towards Implementing a Privacy Policy: An Observation on Existing Practices in Hospital Information System

Suhaila Samsuri<sup>1</sup>, Rabiah Ahmad<sup>2</sup> and Zuraini Ismail<sup>2</sup>

<sup>1</sup>International Islamic University Malaysia (IIUM), Kuala Lumpur, Malaysia,

<sup>2</sup>Universiti Teknologi Malaysia (UTM), Kuala Lumpur, Malaysia

---

## Abstract

In order to safeguard the confidentiality and sensitivity of personal health information belongs to individual, a privacy law is needed to be in place. There are numerous cases of unauthorised intrusions of personal health information occurred but no legal action can be exerted due to the absence of a privacy act in Malaysia. Therefore, a preliminary observation has been conducted to review the current privacy implementations in management of personal health information at Malaysian government hospitals. Analysis was conducted based on OECD Fair Information Practices Guideline which has been the benchmark of most of the privacy and data protection legislation in the world. Interviews were conducted with key personnel in medical informatics and legal expertise using Privacy Impact Assessment (PIA) technique as guidance. The findings of the observation were then compared with the existing health information privacy acts. Then, recommendations were made to include those findings in the proposed privacy law or policy in Malaysia.

**Keywords:** Hospital Information System, Information privacy, Personal Health Information

---

## Introduction

Privacy has eventually gained significant attention from the Malaysian government and hospitals administration with regards to patients' personal health information especially with the government's intention towards a paperless-based information management. Regardless in public or private hospital, privacy and its importance has escalated and requires critical measures to be outlined. It is essential for the Malaysian government to take necessary course of action to develop a legal framework of privacy to curb any manipulation and intrusion of personal health information system. Without doubt, it is a crucial effort to ensure the objectives of patient care enhancement, integrity and

confidentiality are achieved. According to the Ontario Act handbook, a Personal Health Information (PHI) is defined as information that relates to the provision of health care to individuals. In health care terminology, it is commonly referred to an assessment that is done for a health-related purpose and carried out to maintain an individual's physical condition (Cavoukian, 2004). PHI includes oral or written information about individual; relates to the individual's physical or mental health, identification of the individual, family health history, plan of service for long-term care, payment eligibility for health care, individual's substitutes decision-maker, and donation of body parts (Cavoukian, 2004). All these guidelines are necessary in conducting a thorough evaluation of

information privacy practice in Malaysia. Since this is a preliminary stage of research, the following findings are beneficial in the development of the Malaysian comprehensive privacy principles, which in turn can be the base for Asian privacy practice. In developed countries such as the United States, Canada, Australia and New Zealand, the authorities have already instituted its own personal health information protection policies based on its privacy and data protection acts. Only recently, many Asian countries began to relook at privacy issue in a more serious perspective. The enhancement of information technology as well as the globalization process has reshaped the viewpoints of the governments in maintaining the privacy of information from encroachment of unauthorised parties. They also realize that having no specific legislation to protect the privacy of information is a potential pitfall that will cause severe repercussions to the society as a whole. Evidently, the intrusion of patient personal health information has enabled possible attempts by third party to maliciously devastate someone's pride, honour and reputation.

Therefore, it is hopeful that the inference from this research shall drive efforts to develop a PHI privacy preservation guideline for Malaysian Hospital Information System (HIS), in particular. This paper proceeded with relating the previous relevant works done, portrayed in section 2. Section 3 described the methodology used in the observations. The findings are explained in section 4. Section 5 discussed the possibilities of privacy implementation. Finally, section 6 concluded this study.

### **Previous Studies**

Information privacy is about the ability of an individual to control the collection, retention, and distribution of information about him/her (Goldberg *et al*, 1997). In medical practice, information privacy is recognized as the need to communicate information about one's condition and medical history to one's caregivers. An individual expects that access to it will be carefully restricted (Allen, 1995). These definitions obviously conform to the

privacy principles outlined by Organization for Economic Cooperation and Development (OECD) Fair Information Practices Guideline (Cannon, 2005), which has been the base of most health information privacy and data protection legislation in the world, including PHIPA or Personal Health Information Protection Act, 2004 which was enacted based on Canada's Personal Information Protection and Electronic Document Act, 2000 (PIPEDA). It is mainly used in protecting personal health information in the province of Ontario. PIPEDA was developed by using the principles outlined in the OECD Fair Information Practices, which has been improvised to be more consent-based act (Information and Privacy Commissioner). Another example is the New Zealand's Health Information Privacy Code (HIPC) of 1994. The HIPC sets specific rules for agencies in the health sector to ensure the protection of individual privacy remain intact. The code addresses how the health information be collected, used, held and disclosed by health agencies. The difference of HIPC compared with other privacy acts is the degree of its concentration on the purpose of information collected rather than consent. Much emphasis is given to the reason of collecting the information and the openness of the information management (New Zealand Privacy Commissioner).

Although the information privacy principles practiced in these developed countries are likely be the basis of privacy policy in Asian countries, there are principles which certainly do not go well with Asian's norms and practice in privacy. This is mainly attributed to the strong affiliation to a different liberalism which western countries recognized as compared to Asian liberalism. If compared to western individualism concept, Asian cultures are commonly tight with collectivism, grouping concept and non-confrontation; as in Thailand, China, Japan and India (Moore, 1985; Kitiyadisai, 2005; Kumaraguru and Cranor, 2006; Nakada and Tamura, 2005; Adams *et al*, 2009). Individuals in collectivism society usually place more trust and faith in people within their communities rather than those in individualist societies and afraid of being excluded (Hofstede, 1991; 2006). Thus,

authorities and lawmakers must assimilate the local elements of privacy as well as pay much attention to these contradictions during the developmental stage of health information privacy guidelines. In 2005, Taiwan had proposed the draft of framework called 'Medical Information Security and Privacy Protection Guidelines' (Yang *et al*, 2006). Instead of using Fair Information Practices as a guideline, the framework utilized U.S. HIPAA as a benchmark in evaluating their security and privacy principles. The purpose of this guideline is to ascertain what constitutes an effective legal framework in electronic medical records, which will live up to the expectations of healthcare professionals, medical informatics experts and the general public in protecting the privacy of health information.

For the purpose of this study, the OECD Fair Information Practices (FIP) guideline is used as the benchmark in analyzing the information privacy principles practiced in Malaysia's hospitals. FIP is a set of internationally recognized practices in handling the privacy of information about individuals. Information privacy is an important subset of privacy because it provides the underlying policy for many national laws addressing privacy and data protection matters. The first FIP was codified in 1973 by U.S. Department of Health, Education and Welfare in the report entitled; *Records, Computers and the Rights of Citizens* with only five fundamental principles. Then, privacy laws spread to other countries in Europe, which international institutions took up privacy with a focus on the international implications of privacy regulation. In 1980, the Council of Europe adopted a Convention for the Protection of Individuals with regards to Automatic Processing of Personal Data (Council of Europe, 1981). Simultaneously, the OECD proposed similar privacy guidelines in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD, 1980). The OECD Guidelines, Council of Europe Convention, and Europe Union Data Protection Directive (European Union Data Protection Directive) also relied on FIPs as core principles. The principles that made up the guidelines are; accountability, collection limitation, data

quality, individual participation, openness, purpose specification, security safeguards and limitation use (Cannon, 2005). Most of data protection legislation is largely based on the OECD Privacy Guidelines such as EU Data Protection Directive and Asia-Pacific Economic Corporation (APEC) Privacy Framework. Although the U.S. has accepted the OECD guidelines as well, there are significant differences between the EU and APEC approaches to data protection. Since the concept of 'data protection' and 'privacy' are derived from national legal culture and tradition, the application of the regulations varies considerably around the world, even in systems that accept the same fundamental principles (Kuner, 2009).

## **Methodology**

This qualitative preliminary study does not investigate the procedures of PHI management in Malaysian government hospitals only but also intends to understand the society's cultures and its impact on privacy. It was a cognitive evaluation to check the feasibility of the research that will lead to the next comprehensive privacy protection guideline that suits the Malaysian culture. The methods of investigation conducted were adjusted from UK's three main procedures (Warren *et al*, 2008);

- i. The analysis was referred to relevant legislation and policy – OECD Guidelines, PHIPA and HIPC.
- ii. The interviews were selectively conducted with authorized personnel who are directly related to policy practice and data protection in the government and possess hands-on experience in matters related to hospital privacy and data protection policy.
- iii. A limited number of interviews were also conducted to gauge the practitioner perspective and interviewees were chosen among whom have sufficient knowledge in privacy policy and involved in the development of Patient Record Management System.

The health information system in Malaysian government hospital is a

publicly funded system with path and policy determined solely by the Ministry of Health (MOH). Thus, much of the decisions are top-down from the government. In contrast, semi-government hospitals are the ones which are normally under the administration of medical faculties of public universities, specifically providing the in-house training and job opportunity for undergraduates of the same universities including medical and information technology disciplines. Unlike

full government hospitals where external vendor manages the information system, it is quite normal for semi government hospitals' health information systems are managed by their own.

The personnel interviewed were chosen from nationwide to cover wider range of responsibilities; Information Technology Director and Officer, Electronic Medical Record Officer and magistrate; as shown in Table 1.

**Table 1: Pilot Study Interviewee**

Designation	Number of interview	Organization
<b>Information Technology Director</b>	1	MoH
<b>Information Technology Officer (involved in Malaysia Hospital Information System)</b>	1	MoH
<b>Electronic Medical Record Officer</b>	1	Government Hospital
<b>Electronic Medical Record Officer</b>	1	Semi-government Hospital
<b>Magistrate</b>	1	Malaysian Magistrate Court

5 interviews were conducted in November 2009, whereby each session took 45 to 50 minutes to complete. The designs of the questionnaires were adapted from the Privacy Impact Assessment (PIA) questionnaires module;

- Privacy Impact Assessment Guidelines: A Framework To Manage Privacy Risks (Treasury Board of Canada Secretariat, 2002)
- Privacy Impact Assessment Process (PIA) (Ministry of Labour and Citizens' Services)

This paper presents the preliminary results of the study and shall form an integral part in the development of Malaysia's health information privacy policy. A comprehensive research on developing the above shall be conducted at a later stage and more significant findings will be deduced from a more refined data.

## Result

Some government hospitals have adopted a Patient Management System (SPP) for

managing their patients' records. Despite that it is still a pilot test, its primary objective is to install that into each government hospital in the future, upon MOH's approval. Other government hospitals are using their own health information systems that suit their management requirements but strictly under the control and restriction by MOH policies. To date, Malaysian hospitals do protect the patient's health information under a principle called 'duty of care'. It is a legal principle which is defined as a duty to take reasonable care to avoid acts or omissions which you can reasonably foresee that would be likely to injure persons who are so closely and directly affected by your act or omission that you ought reasonably to have them in contemplation as being so affected when directing your mind to the act or omission in question (Treasury Board of Canada Secretariat, 2002). By a simple definition, 'duty of care' stipulates the obligation that one party should hold towards another while under its responsibility. In other words, the hospital or health care provider is liable to provide reasonable care to its

patient and their personal information, regardless of their age, ethnicity, status and so forth. As clearly said by a legal expert:

*"Duty of Care principle is merely a legal maxim which is not tantamount to an enforceable law; it is foreseeable that the intrusion of PHI will continue to happen. Patients would not be able to build up their case for damages and compensation should the hospital is able to display a reasonable duty of care was exercised accordingly" (Magistrate).*

Clearly, Malaysia needs an act that specifically addresses personal health information protection as 'duty of care' alone is insufficient to discourage any serious intrusion of personal health information at hospitals. Moreover, the proposed act must at least cover the privacy principle requirements listed below. The interview's findings were arranged based on eight components in OECD Guidelines. The following are statements in support of the various principles commonly required for information privacy preservation.

- Privacy principle 1 - Accountability:

Malaysian hospitals already have a systematic information maintenance procedure in ensuring the accountability of personnel managing the PHI being collected. Staffs tasked to perform the duty are provided with adequate hands-on training and knowledge in handling all PHI issues including access, collection, transmission, storage and disposal of PHI. As an officer claimed,

*"All staffs, including doctors, nurses and officers involved with the system usage and maintenance are well-trained and provided with appropriate courses to handle any new installed system"(Officer 1).*

- Privacy principle 2 - Limited Collection of PHI:

Collection of personal health information was obtained directly from the individual patient itself or his/her authorized representative.

- Privacy principle 3 - Data Quality:

The patient's records system management has its specific procedures to be adhered to ensure that PHI is accurate, complete and up-to-date, along with the log records which indicate the last information update. The patients are permitted to rectify any errors in their PHI by informing the hospital staffs only, but limited to non-critical information such as address, phone number and date of birth. Other critical information such as laboratory test results, vaccinations, surgeries, illnesses and hospitalization, medications, allergies, other procedures and so forth are subjected to doctors' authorization for amendments. According to the officer;

*"There are two types of personal information in a hospital; critical and non-critical health information. Critical information commonly includes treatment, diagnosis and medicine prescription. While non-critical information include name, age, I/C number, income, ethnic and social status. Patients are only allowed to make corrections on non-critical health information" (Officer 1).*

- Privacy principle 4 - Individual Participation:

This principle is divided into two aspects namely patient consent and access to their PHI as stated in the principles of PHIPA and code of HIPC. The existing privacy policy in Malaysian hospital has little concern for patient permission and consent over their own PHI. Very often, no notice or specific procedures are available in displaying the purpose of collecting information other than commonly acknowledged. It is assumed that the patients has consented the information collection. Since the patients have never been informed of any specific secondary usage of the information, there is no necessity to give an opportunity for an individual to grant their consent for any use of information other than commonly known. There is no documented procedure being displayed for any confidential communications request. An officer said,

*"Secondary usage for evaluation and forecasting are very important for the improvement of hospital service in the future. It is generally understood that the patients willing to grant their trust towards government information management, which the collection only related to the benefit of hospital. It is very rare to be questioned by patients concerning the usage of their PHI so far" (Officer 2).*

The health information systems designs in Malaysian hospitals are unfriendly to patients who like private accesses to their own personal health information. There is no online system or intranet for public access to hospital internal network access of PHI. Patients who desire to check or obtain a copy of their PHI will have to forward their request to the patient record management counter. This has been classified as a weakness and currently under the concern of semi government hospitals' management for upgrading.

- Privacy principle 5 – Openness:

There is a lack of transparency in cascading the complete policies in managing PHI to patients. There is a need to insist on hospital management to display necessary information such as privacy policy, PHI management procedures and patients' rights. Unfortunately, much consideration in terms of financial implications incurred by the hospital and government must be taken into account, before this request is entertained. As one of the interviewees said,

*"This is a non-profit based government organization, where people come most of the time without incurring any cost on their side at all (for low-income community). We (government) spent for them. They are already grateful enough to be treated and cured" (Officer 1).*

- Privacy principle 6 - Purpose specification:

Collection of personal health information was strictly related to the purpose and needs of medical activities such as evaluation, medical research, case study,

development or forecasting which is secondary.

- Privacy principle 7 - Storage and Security of PHI:

Malaysian hospitals are found to be conscious on the security of PHI storage with the provision of specific procedures for its collection, access, storage and disposal. The electronic patient records systems also been accommodated with privacy access mechanism that allowed only authorized staffs to control access and changes to PHI using user ID and password. The authorization is granted strictly for the purpose of 'need to know' basis or medical activities for which it is collected. There are special securities mechanisms embedded for the high sensitive information, such as, HIV, DNA and so forth, which need more privacy protection.

*"The authorization is granted on role and need-to-know basis using a particular password and the access to patient sensitive records are more restricted" (Officer 1).*

The fact that most information systems operating in Malaysian hospitals are mostly developed by information technology vendors yields a necessity to hospital management or MOH itself to set a certain standards of agreement with vendors, with regards to preserving the confidentiality of patient's health information.

*"It is understandable that most vendors may refuse to disclose the full source codes and configuration on the system for hospital future maintenance works and modification. Besides maintaining their exclusive rights on the system, they also have a standardized system design and not customized only for the use of certain type of hospitals only" (Officer 2)*

Even though there is a possibility for them to have online communication, patients still will not be able to fully control over third party access of their critical information. An officer claimed,

*"We are developing our own health information system to improve security and*

*privacy control over health information management and to avoid any vendor's involvement. Patients will have the chance to access their own PHI and make amendment to non-critical PHI only" (Officer 4)*

- Privacy principle 8 - Limited usage, disclosure and retention of PHI:

The usage, disclosure and retention of PHI are limited only for the purpose of information collection or reasonable circumstances for the benefit of person's health. This information will only be used in that hospital itself or hospitals within Malaysia. An officer said,

*"There is no purpose other than medical activities for patient information collection" (Officer 2).*

## Discussion

The PHI management in Malaysia can be described as, to a certain extent, to be secured and reliable, although more adequate measures must be available to deter possible intrusion of privacy. The visible weaknesses mostly found in the patients' rights and participation, such as patient's self-access right and full control on their own PHI as practiced by PHIPA in Ontario, which is more on consent-based. Another weakness is the lack of openness of hospital PHI maintenance procedures as practiced by HIPC in New Zealand. Although Malaysian hospitals are ambitious to move towards a paperless administration, it is important to note that the system structure, plan, design and implementations are specifically for the hospital management only with less consideration given to the patients' convenience and utility. Until to date, there is no proposed online system which will provide patients with free self-access of their PHI. Patients are given rights to check, amend or argue on what are recorded in their PHI but their accesses are not granted. Although there is no serious demand from the patients to exercise their privacy rights especially in the government hospitals, the hospital management should not ignore this responsibility. Information privacy is important in government

hospitals, in order to maintain good reputation in the public perception. The adoption of information privacy principles in hospitals' Health Information System (HIS) especially in handling personal health information must benefit both hospital management and the patients themselves. This is particularly vital in improving the trust and confidence of the patients. It is also unequivocal for the hospital management to mitigate any possible unethical deeds; such as identity theft, patient information leakages and loss and unauthorized modification of PHI.

When arguing on the readiness of adopting health information privacy act for Malaysia, one interviewee noted that:

*"Malaysia should start developing their own information privacy act that suits with our environment, in order to cope with global privacy trend. It can be one of the important factors to gain trust and confidence from foreign investor and tourists, since Malaysia are improving its global economic activities including health tourism sector" (Officer 1)*

The second officer however remarked,

*"Malaysia is perhaps not fully ready for the full implementation of privacy according to western concept. We are unique societies where distinction gap in social cultures and values co-exist, unless the modification is done for the privacy concept to suit us" (Officer 2).*

The situation in Malaysia may suit the argument by Moore (Moore Jr, 1985) about Asian concept of privacy,

*"The desire for privacy, in the sense of protection or escape from other human beings, emerges when an individual becomes subject to social obligations that individual cannot meet or does not want to meet. On the other hand, this desire for privacy can evaporate if the person develops a feeling of dependence on the people who are the source of the onerous obligations."*

Moore's theory added that privacy cannot be the dominant value in their society

(Moore Jr, 1984), due to the multi-cultures and believes issues.

## Conclusion

This paper has successfully made a comparison between a standard management of PHI in Malaysian government hospital against the OECD Fair Information Practices Guideline and other two health information privacy principles from PHIPA and HIPC. In doing so, this paper tried to avoid being hypercritical on the advantages or disadvantages of the existing acts practiced by the developed countries since the enforcement of the respective acts is based on respective needs and requirements of their particular countries and environments. As for Malaysia, it is recommended that the three stated missing principles; patient consent, patient free accessibility and transparency in PHI management must be included in privacy policy. The authority and lawmakers also have to carefully design its PHI policy to correspond with its uniqueness in terms of multi-ethnicity, multi-religion, multi-cultures and values. Instead of adopting the concept of consent-based from PHIPA or purpose and openness-based from HIPC, Malaysia is likely to be more trust-based concept, where patients put more confidence and trust on hospital management to handle their PHI. The future work on the development or implementation of the policy will take those into consideration to avoid any unnecessary dissatisfaction by certain quarters. It would be appropriate to examine other Asian countries like Japan, China, Thailand and India in handling privacy issues. All of the above indicate that it is pertinent for Malaysia to quickly devise its own standard of privacy rules for PHI management to protect the confidentiality of its citizen's personal health information. In addition to that, it is essential for the government to demonstrate its efforts to build trust among the people towards government management system. This in-progress study will proceed to the actual research in designing Malaysian PIA concept, which will be used in developing the Malaysian PHI management system in HIS.

## References

- Adams, A. A., Murata, K. & Orito, Y. (2009). The Japanese Sense of Information Privacy, *AI & Society*, vol. 24, pp. 327-341
- Allen, A. L. (1995). "Privacy in Health Care," Reich WT, ed. Encyclopedia of Bioethics, vol. 4, pp. 2064-2073, NY: Macmillan
- Cannon, J. C. (2005). Privacy: What Developers and IT Professionals Should Know, Addison-Wesley, pp. 45
- Cavoukian, A. (2004). "A Guide to the Personal Health Information Protection Act," *Information and Privacy Commissioner of Ontario*: 46
- Goldberg, I., Wagner, D. & Brewer, E. (1997). "Privacy-Enhancing Technologies for the Internet," Proceedings, *IEEE COMPON'97*, pp. 103-109
- Hofstede, G., "Geert Hofstede Analysis," [Online], [Retrieved on January 2010]. [http://www.cyborlink.com/besite/hofsted\\_e.htm](http://www.cyborlink.com/besite/hofsted_e.htm)
- Hofstede, G. (1991). Cultural and Organizations - Software of the Mind - Intercultural Cooperation and its Importance for Survival. McGraw-Hill
- Information and Privacy Commissioner/Ontario [Online], [Retrieved on January 2010] [http://www.elaws.gov.on.ca/html/statutes/english/elaws\\_statutes\\_04p03\\_e.htm](http://www.elaws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm)
- Kitiyadisai, K. (2005). Privacy Rights and Protection: Foreign Values in Modern Thai Context. *Ethics and Information Technology*, vol. 7, pp. 17-26
- Kumaraguru, P. & Cranor, L. (2006). Privacy in India: Attitudes and Awareness. Danezis, G., Martin, D. (Eds.). *PET 2005, LNCS*, vol. 3856, pp. 243-258
- Kuner, C. (2009). An International legal Framework for Data Protection: Issues and Prospects, *Computer Law & Security Review*, vol. 25, pp. 307-317

Ministry of Labour and Citizens' Services,  
Privacy Impact Assessment Process (PIA).  
[Online], British Columbia, [Retrieved on  
January 2010]  
<http://www.cio.gov.bc.ca/services>

Moore Jr, B.(1984). Privacy: Studies in  
Social and Cultural History. Armonk, New  
York

Moore Jr, B. (1985). Privacy, pp. 287-299

Nakada, M. & Tamura, T. (2005). Japanese  
Conceptions of Privacy: An Intercultural  
Perspective. *Ethics and Information  
Technology*, vol. 7, pp. 27-36. Springer

New Zealand Privacy Commissioner  
[Online], [Retrieved on January 2010]  
<http://www.privacy.org.nz/health-information-privacy-code/>

Treasury Board of Canada Secretariat  
(2002). Privacy Impact Assessment  
Guidelines: A Framework to Manage  
Privacy Risks, [Online], [Retrieved on  
January 2010]  
[http://www.tbsst.gc.ca/pubs\\_pol/ciopubs/pia-pefr/paipg-pefrld-eng.asp](http://www.tbsst.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld-eng.asp)

Warren, A., Bayley, R., Bennett, C.,  
Charlesworth, A., Clarke, R. & Oppenheim,  
C. (2008). "Privacy Impact Assessments:  
International Experience as a Basis for UK  
Guidance," *Computer Law & Security  
Report*. Vol 24, pp. 233-242

Yang, C.-M., Lin, H.-C., Chang P. & Jian, W.-S.  
(2006). "Taiwan's Perspective on  
Electronic Medical Records' Security and  
Privacy Protection: Lessons Learned from  
HIPAA," *Computer Methods and Programs  
in Biomedicine*, vol. 82, pp. 277-282