**International Journal of Information Security and Privacy**
Volume 17 • Issue 1

# Legal Compliance Assessment of the Malaysian Health Sector Through the Lens of Privacy Policies

Ali Alibeigi, University of Malaya, Malaysia*
Abu Bakar Munir, University of Malaysia, Malaysia
Adeleh Asemi, University of Malaya, Malaysia

## ABSTRACT

Value of information privacy has changed over time. Hence a weak personal data protection legal system will increase the threats and damages to individuals, especially in case of sensitive data like health information. Considering increasing amount of incidents, there is not any report or study showing how far Health companies protect both personal information of Malaysian citizens. The objective of this study was to assess the level of compliance with Malaysian Personal Data Protection Act 2010 by hospitals, clinics, and pharmacies. The authors used qualitative method using document analysis. The authors evaluated privacy policies of samples in line with requirements of the Act, especially Notice and Choice Principle and rights of individuals. Findings of the study showed serious non-compliance. Some companies are completely unaware of the Act. Considering sensitivity of health information and its value, the authors suggested amending alternatives to be applied for these privacy statements. The authors suggested specific inspections and issuance of guidelines and orders by data protection commissioner.

## KEYWORDS

Access right, Clinic, Hospital, Personal data protection, PDPA, Sensitive data

## Introduction

The increasing cyber threats to individuals' information privacy have encouraged the Malaysian government to enact the Personal Data Protection Act 2010 (PDPA). It was the first personal data protection law among members of the Association of Southeast Asian Nations (ASEAN). PDPA was gazetted on 10 June 2010 and entered into force after three and half year delay on 15 November 2013. The main objective of the PDPA is to protect the personal information of individuals. The PDPA applies to private sectors only and with respect to their commercial activities (Alibeigi, 2020). In Malaysia, information privacy cases are increasing. For instance, the sensitive data of thousands of Malaysian patients were stolen from both government and private hospitals' systems (Personal health data theft scary, 2016). The information has been sold to the pharmaceutical companies. Remarkably, this incident happened 2 years after the enforcement of the Act. Health companies need to collect personal information and medical data of individuals to provide medical services and the PDPA does recognize it. However, they have to observe the requirements provided by the PDPA like the Notice and Choice Principle and individuals' rights over their personal data. Definitely, non-compliance

DOI: 10.4018/IJISP.315818 *Corresponding Author

with the Act, especially for medical information which is categorized under sensitive data will cause serious damages to the data subjects.

The sensitivity of information privacy dangers, especially for the medical information and lack of study on the compliance assessment by health companies necessitates conducting research focusing on this area. Moreover, there is not any official report or study concerning the level of compliance with the PDPA requirements by health companies (hereinafter HC). Hence, this study aimed to assess the privacy policies of health companies including hospitals, clinics, and pharmacies. In fact, we will assess the requirements of the PDPA through the lens of privacy policies.

To conduct this qualitative study, the requirements of the Notice and Choice Principle (hereinafter NCP) and individuals' rights were selected as evaluation factors.[1] Privacy policy (hereinafter PP) is a primary and reliable document and evidence to assess how far a data user may fulfill the requirement of the PDPA. Basically, the PPs play the role of a written notice under the NCP.

Thus, the evaluation from the perspective of privacy policies will clear that how far the rights of data subjects are being respected by a company while collecting and using their personal data. To date, there is no survey or report on the compliance status with the PDPA by the data users. The results of this survey not only provide a compliance awareness for the data users, but also the regulator in his monitoring functions. The research by finding out the non-compliance areas of the PDPA through privacy statements will provide a proper checklist for all present and future data users and processors to be more compliant with the Act. This study can be a warning message for existing companies to rectify the shortcomings of their privacy policies whereas a reference guideline for the newly registered companies to base their privacy approach in a proper position at an early stage. Therefore, the current study sets out the weaknesses of the current trend in the adoption and application of privacy policies by health companies in Malaysia.

## Literature Review

While more than a decade has passed since the enactment of the PDPA, little research has been done concerning its implementation. Moreover, there is not any readiness survey or official report to assess compliance with the Act.

Alibeigi et al. (2021) evaluated the privacy policies of the banks and financial institutions in Malaysia. The results indicate a considerable non-compliance with the principles and requirements of the Personal Data Protection Act 2010 (PDPA) specially Notice and Choice Principle and individual's rights. The result of this qualitative research shows that it is against the PDPA to draft a common privacy policy for all subsidiaries under a group company. They collect excessive data, and even sensitive data and even through unusual measures. Privacy policies provided for vast, unlimited and vague purposes of data collection. Sharing of data with third parties, other subsidiaries under a parent company and also sending of data abroad to unknown processors are evident. Alibeigi et al. (2022), assessed the level of compliance with the PDPA requirements through privacy statements of Communications industry. According to them, 80% of companies provided for an easy access to their online privacy policy and 50% drafted a lengthy privacy policy. 35% collect sensitive data, all share the personal data with the third parties and 85% provided for a vague specification of the third parties. Only 25% provided a clear method of access right to personal data, 45%s have facilitated the correction of data request by special mechanism. 25% have appointed a Privacy Officer with contact information. Majority provided for a clear and limited purpose(s) for data collection. They have suggested for a standard model to modify the present privacy policies, recommendations for Data Protection Commissioner and also amendment of the Act.

Industry Readiness Survey (2014) by SPDPC aimed to assess the "awareness and readiness of organizations in preparing for compliance with the Personal Data Protection Act" (SPDPA). 65.8% of the organizations more or less were aware of the 9 data protection obligations, 50.7% have provided data protection measures, and 50.1% of them were clear on compliance with the SPDPA. "Industry

Relationships between Information Security Concerns and National Cultural Dimensions: Findings in the Global Financial Services Industry

Princely Ifinedo (2011). *Security and Privacy Assurance in Advancing Technologies: New Developments (pp. 134-153).*

www.irma-international.org/chapter/relationships-between-information-security-concerns/49500