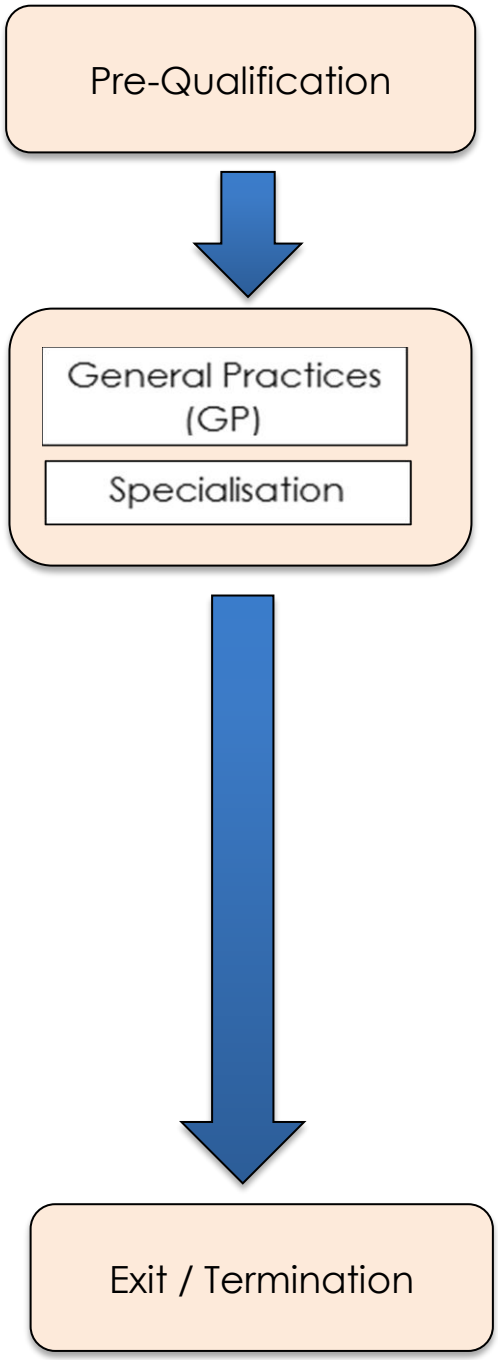

1. Inadequate quality control of private colleges providing health sciences education
2. Supplies of clinical training for housemen and nursing

2. Lack of Regulatory Framework for MCO Operation
- Minimal fees paid to medical professionals
- Intervention on clinics operation
- Delayed and partial reimbursement
- Selective Empanelling and Fee Splitting

3. Discrepancies between Personal Data Protection Act 2010 and PHFSA 1998
- The Redundancy on Confidentiality
- Difficulties to gain access of data of Information

7.0 Personal Data Protection

7.1 Discrepancies between *Personal Data Protection Act 2010* and *PHFSA 1998*

a) The Redundancy on Confidentiality of Information

Personal Data Protection Act (PDPA) 2010 regulates the collection, recording, holding or storing of personal data, and carrying out of any operation on personal data for commercial transactions. The Act, however, does not restrain a party from processing data if the processing is done legitimately, in accordance with its principles. The Act does not apply to Federal and State Governments; non-commercial transactions; personal, family and household affairs; credit reference agencies; personal data processed outside of Malaysia (unless the data is intended to be further processed in Malaysia).

The PDPA categorizes data as follows:-

1) Personal data: means any information in respect of commercial transactions, which—

   (a) is being processed wholly or partly by means of equipment operating automatically in response to instructions given for that purpose;
   (b) is recorded with the intention that it should wholly or partly be processed by means of such equipment; or
   (c) is recorded as part of a relevant filing system or with the intention that it should form part of a relevant filing system,

   that relates directly or indirectly to a data subject, who is identified or identifiable from that information or from that and other information in the possession of a data user, including any sensitive personal data and expression of opinion about the data subject; but does not include any information that is processed

for the purpose of a credit reporting business carried on by a credit reporting agency under the *Credit Reporting Agencies Act 2010*;

2) Sensitive personal data: means any personal data consisting of information as to the physical or mental health or condition of a data subject, his political opinions, his religious beliefs or other beliefs of a similar nature, the commission or alleged commission by him of any offence or any other personal data as the Minister may determine by order published in the *Gazette*;

PDPA is seen by practitioners as an **additional burden and redundant** as it has already been addressed under the *Private Healthcare Facilities and Services Act* (PHFSA) 1998. In addition to PDPA, registered medical practitioners have to abide by the Malaysia Medical Council (MMC) guidelines which are the code of professional conduct and the confidentiality guidelines for medical practice. The medical practitioners, especially those operating small clinics, are concerned that the need to apply with to the PDPA will involve more documentation and application fees.

One of the redundancies between PDPA with PHFSA and The Confidentiality Guidelines is the method used to safeguard the confidentiality of information. Box 7.1 highlights the data protection clauses that guide data user on how to secure information of the data subject.

BOX 7.1 : The Redundancy on Confidentiality of Information

1) *Private Healthcare Facility Services Act 1998*

Section 115

(1) Every person employed, retained or appointed for the purpose of the administration or enforcement of this Act **shall preserve secrecy with respect to all information that comes to his knowledge in the course of his duties and shall not communicate any information to any other person**

(a) to the extent that the information is to be made available to the public under this Act;

(b) in connection with the administration or enforcement of this Act or any proceedings under this Act;

(c) in connection with any matter relating to professional disciplinary proceedings, to a body established under any law regulating a health profession;

(d) to the person's counsel, upon the person's request where the information relates to any healthcare service provided to him; or

(e) with the consent of the patient or legal guardian to whom the information relates.

(2) Any person who contravenes subsection (1) commits an offence and shall be liable on conviction to a fine not exceeding one thousand ringgit.

2) *Personal Data Protection Act 2010*

Section 9

A data user shall, when processing personal data, **take practical steps to protect the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction**

3) The Confidentiality Guidelines by MMC

Paragraphs 10

When **a practitioner** is responsible for personal information about patients, the practitioner shall ensure that **the information and any documentation about it are effectively protected against improper disclosures at all times**

b) Difficulties to gain access of data

Consent is considered as a major factor of the PDPA 2010. The medical professionals brought up their concern on the stringent data control in the PDPA where only the data subject has access to his/her information or could give consent to other data user requiring the information. This is as per Section 39 of the Act:

Personal Data Protection 2010

Section 39

Personal data of a data subject may be disclosed by a data user for any purpose other than the purpose for which the personal data was to be disclosed at the time of its collection or any other purpose directly related to that purpose, only under the following circumstances:

(a) **the data subject has given his consent to the disclosure**

7.2 The objective of the Act

Through the enforcement of PDPA 2010 (Security Principle), the data user believed that they have to change the way they handle customers' personal data. Security Principle in PDPA is considered as the most challenging principle in processing personal data since the businesses have to take practical steps to protect the personal data from any loss, misuse, modification, unauthorised or accidental access or disclosure , alteration or destruction[1]. Despite of that, the implementation of PDPA will increase the cost in protecting the data since businesses have to use effective security measures and proper tools to protect the personal data from being disclosed to an unauthorised party unwillingly[2]. The relevant information of the Act is illustrated in Box 8.8 below.

[1] See article from Taylor Wessing (May 2014) (http://www.taylorwessing.com/globaldatahub/article_malaysia_dp.html)

[2] See the article in The Star Online (2 February, 2014) (http://www.thestar.com.my/News/Nation/2014/02/02/Businesses-in-the-dark-over-the-PDPA/)

Box 7.2 : Personal Data Protection Regulations 2013

Part II : Personal Data Protection Principles
Security policy

6. (1) The data user shall develop and implement a security policy for the purposes of section 9 of the Act.
   (2) The data user shall ensure the security policy referred to in sub-regulation (1) complies with the security standard set out from time to time by the Commissioner.
   (3) The data user shall ensure that the security standard on the processing of personal data be compiled with by any data processor that carry out the processing of the personal data on behalf of the data user.

7.3 Verification with Regulators

Based on the issues discussed, a verification session was conducted with regulators, Personal Data Protection Department (PDP) team. It was made to understand that the department has provided a robust and dynamic approach to the PDPA where industries are consulted in the development of Code of Practice that meets the customised requirements of individual industry. To date, four industries have established their code of practice under the PDPA, namely Banking, Utility, Insurance and Communication.

According to the regulator, PDPA can be designed to ease the process of data protection for business owner despite the issues raised by Medical Professionals with regards to unnecessary burdens cause by it. PDPA is an industry driven Act and it promotes self-regulation that can be customised based on industry requirement as stated under ***Section 23 of PDPA: Code of Practice.*** The PDPA also stated that the data user shall develop and implement a security policy for the purpose as long as it complies with the security standard set out from time to time by the Commissioner.

The PDPA emphasizes on the accountability of medical professionals over data subject information, however, it does not dictate the process of storing data/file/patients' record as mentioned in ***Section 9 of PDPA: Security Principle***. In summary, the section stated that a data user shall, when processing personal data,

take practical steps to protect the personal data from any loss, misuse, modification, unauthorized or accidental access or disclosure, alteration or destruction. The PDPA addresses the limitation faced by industry player's especially small clinics with limited resources. Therefore, PDPA allows any form of unique treatment to data as long as the information is safely maintained and the data processer provides sufficient guarantees and security measures.

According to the PDP department, most private hospitals are keen to register with PDPA and to date, over 3000 private hospitals have registered as data user and/or processor. However, the number of small clinics registering with the PDPA remains minimal. Most established private hospitals see PDPA as a good assurance of protecting customer's data thus strengthening the marketability of their services, especially to international patients seeking medical treatment in Malaysia. The PDPA is also relevant with the government's initiative to double the revenue of medical tourism from RM 688 million to over RM1 billion in 2020.

The Personal Data Protection Department however faces challenges in developing the code of practice for healthcare industry. The meeting set on 12 December 2015 has been postponed to January 2016, delaying the process much further. The PDP department believes that the PDPA is very much relevant to the healthcare industry based on the high level of data sensitivity. They also believe that the code of practice would ease the registration and PDPA implementation of over 8000 private clinics as it provides guidelines that cater specifically to the industry's environment.

Redundancy on disclosures of the information

The investigation revealed that there is a misunderstanding with regards to the requirements of PDPA against the medical professionals Act and PHFSA and that the issue of redundancy of protection of information is not valid. That is because, although the *Medical Act 1971* states the necessity to protect patient's data, it however does not outline detail aspects of personal data protection as recognised by international

industry players. The Medical Industry practitioner may design their own methodology of data protection including storage and administration of patient's data to specific suitability of the industry players, including private hospitals and small private clinics.

The customised guideline could be incorporated into the Code of Practice for the Healthcare Industry of the PDPA, as established by the Banking, Utilities, Insurance and Communication Industries. It could be designed to ease the way of doing business, enhance patient's confidence in clinics and private hospitals data administration thus strengthening the marketability of practices. Therefore, the Medical Industry players should adopt a far-sighted approach and act fast to initiate the development of the Code of Practice under the PDPA.

The PDPA also helps to establish greater confidence to the international industry players as the clauses weighs down the impact of non-conformance to the Act. The PHFSA stated that any person who contravenes the Act (Section 115 (2)(1)) commits an offence and shall be liable on conviction to a fine not exceeding one thousand ringgit while under the PDPA a person who contravenes the Act (Section 40 (3)(1)) commits an offence and shall, on conviction, be liable to a fine not exceeding two hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both. That provides bigger protection to data subject and the confidentiality of his/her medical information.

The principles of data treatment and security are well covered under the PDPA as it also conceals a bigger spectrum of the industry. On the other hand, the Medical Act and PHFSA did not emphasize on such. The revised guidelines on Confidentiality Guidelines published by the MMC on October 2011 meanwhile focuses only on the liability of Doctors who are registered with MMC in protecting and sharing patient's information. It does not cover other employees or data processors who are not registered with the MMC. Moreover the guideline which is tied to the *Medical Act 1971* imposes only minimum penalty to non-compliance and may not pose as a good measure to deter noncompliance.

Table 7.1 illustrates the Comparison on data protection clauses stated in the Confidentiality Guidelines by the MMC, *Private Healthcare Facilities and Services Act 1998* (PHFSA) and the *Personal Data Protection Act 2010* (PDPA) :

Table 7.1: Comparison on data protection between Confidentiality Guidelines, Private Healthcare Facilities and Services Act and PDPA Act.

Confidentiality Guidelines - MMC	PHFSA (Ministry of Health, MOH)	PDPA (PDP Department)
Overall Guidelines mention about how doctors registered with MMC are liable to data protection Clause stating all medical **practitioners registered with MMC : automatically refer to doctors only** Data protection: electronic etc. Sharing patients' info: Consent, How to share, with whom can share.	**Section 115. Confidentiality of Information** (1) Every person employed, retained or appointed for the purpose of the administration or enforcement of this Act shall preserve secrecy with respect to all information that comes to his knowledge in the course of his duties and shall not communicate any information to any other person except - (a) to the extent that the information is to be made available to the public under this Act; (b) in connection with the administration or	**Section 40. Processing of sensitive personal data** (1) Subject to subsection (2) and section 5, a data user shall not process any sensitive personal data of a data subject except in accordance with the following conditions: (a) **the data subject has given his explicit consent** to the processing of the personal data; (b) the processing is necessary – (iv) for medical purposes and is undertaken by— (A) a healthcare professional; or (B) a person who in the

Confidentiality Guidelines - MMC	PHFSA (Ministry of Health, MOH)	PDPA (PDP Department)
	enforcement of this Act or any proceedings under this Act; (c) in connection with any matter relating to professional disciplinary proceedings, to a body established under any law regulating a health profession; (d) to the person's counsel, upon the person's request where the information relates to any healthcare service provided to him; or (e) **with the consent of the patient or legal guardian** to whom the information relates. (2) Any person who contravenes subsection (1) commits an offence and shall be liable on conviction to a fine not exceeding one thousand ringgit.	circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a healthcare professional; (3) A person who contravenes subsection (1) commits an offence and shall, on conviction, be liable to **a fine not exceeding two hundred thousand ringgit or to imprisonment for a term not exceeding two years or to both.**

In addition, the Act also governs the practice of third party data processor acting on behalf of data user (medical professional) as stated in Section 9 of the Act "The data user shall ensure that the security standard on the processing of personal data be compiled with by any data processor that carry out the processing of the personal data on behalf of the data user". That provides better protection to data subject whist increasing patients' confidence to seek treatment in PDPA registered clinics and hospitals. Such a clause however does not exist in the PHFSA nor the other existing guidelines on the administration of patients' data.

Restriction in Accessing Patient's Data

The verification session with the regulator and further studies on the PDPA Act has confirmed that there is an element of serious restriction where only data subject could give consent to data release.

One medical practitioner shared that parents of a deceased child has not been given the permission to access their child's medical history record as there was no consent given by the deceased, who died at the age of above 18. Data however could only be released under the court order as stated in Section 39 of the Act. However, the "Extend of Disclosure of Personal Data" but would involve lengthy legal processes and high cost.

Box 7.3 : Personal Data Protection Regulations 2010

Section 39 : Extend of Disclosure of Personal Data Notwithstanding section 8, personal data of a data subject may be disclosed by a data user for any purpose other than the purpose for which the personal data was to be disclosed at the time of its collection or any other purpose directly related to that purpose, only under the following circumstances: (a) the data subject has given his consent to the disclosure; (b) the disclosure —

(i) is necessary for the purpose of preventing or detecting a crime, or for the purpose of investigations;
or
(ii) was required or authorized by or under any law or by the order of a court;
(c) the data user acted in the reasonable belief that he had in law the right to disclose the personal data to the other person;
(d) the data user acted in the reasonable belief that he would have had the consent of the data subject if the data subject had known of the disclosing of the personal data and the circumstances of such disclosure; or
(e) the disclosure was justified as being in the public interest in circumstances as determined by the Minister

This restrictions have caused a regulatory and administrative burden to medical professionals as whether to comply to the PHFSA 1998 and Code of Professionals Conduct, which provides better flexibility where the data user could request the consent from the data subject or **a person authorized to Act on the patient's behalf** for any disclosure of information, or comply to the PDPA's restriction.

The related clauses under the relevant Acts and guidelines are highlighted in Box 7.4.

BOX 7.4 : Disclosures of the information

1) ***Private Healthcare Facility Services Act 1998***
Section 115, Subsection 1(e)
With the consent of **the patient or legal guardian** to whom the information relates.

2) The Confidentiality Guidelines
Paragraph 21
A practitioner may release confidential information in strict accordance with the **patient's consent or the consent of a person authorized to act on the patient's behalf**. Seeking patient's consent to disclosure of information is part of good medical practice.

The Code of Professional Conduct 1986 however does not specify the role of any authorised person to act on behalf of the data subject as stated in the **Code of Professionals Conduct** Subsection 2, which stated that “A practitioner may not improperly disclose information which he obtained in confidence from or about a patient”. This gives flexibility to medical practitioners to obtain consent for patient’s data release from the legal guardian or other authorised person. This is especially relevant for patients under 18, as stated in Section 24 of the *Child Act 2001* as illustrated in Box 8.7.

7.4 Options to resolve the issues

The following options are put forward to resolve the issues of redundancy in the PDPA implementation:

1. Status quo

   PDPA remains in action without any changes to the principles of the Act. That is because there is no redundancy in the manner of protection data in the PDPA against the PHFSA. The issue was raised mainly due to lack of understandings by businesses on the purpose of the Act or what they are required to do.

2. Expedite the development/establishment of Code of Practice
   - Benefit: PDPA that supports the industry
   - Addresses concerns & limitations
   - Managing business compliance costs across the board

3. Strengthen communication to establish better understanding of PDPA among medical professionals. This must be done after the establishment of code of practice.

7.5 Recommended options

It is recommended that all options be implemented due to the followings:

Option 1: There is clearly no redundancy in the PDPA against the existing PHFSA Act. The PDPA was developed to provide a holistic guideline to data protection involving data subject, data user and data processor. However the PHFSA only addresses specific areas of data protection which does not include the manner to process, secure and store data. The PHFSA also does not mention of any liability of third party data processor acting on behalf of data user. Hence, the PDPA does not contradict of pose redundant to the PHFSA.

Option 2 is also recommended to complement Option 1. That is because the development/establishment of Code of Practice would provide medical professionals with a specific guideline on data protection that is customised to the Healthcare Industry. The Code of Practice would address needs and limitations of medical practitioners in processing, storing and securing patients' data especially for those operating small clinics. The Code of Practice will also provide every party (data subject, data user, processor) a clear picture in determining the objective of secrecy of the data. With this in mind, the appropriate policies and procedures regarding the collection, processing, retention and disclosure of personal data can be implemented[3].

To compliments options 1 and 2, the PDP Department is recommended to strengthen communication with industry players, particularly medical practitioners operating small clinics. Apart from communication, the Department could take a proactive role by developing independent data processors who are able to process data in accordance to the PDPA requirements. These trained data processors could support the administrative data management function for small clinics based on outsourcing services. This would ease the transition for small clinics into PDPA. This approach has been successful based on the experience of the Custom Department in easing the implementation of the Goods and Services Tax (GST) throughout 2014 to 2015.

[3] See article form HG.org (http://www.hg.org/article.asp?id=33273)