APHM
Persatuan Hospital Swasta Malaysia
Association of Private Hospitals of Malaysia

CODE OF PRACTICE

FOR PRIVATE HOSPITALS IN THE HEALTHCARE INDUSTRY

(Pursuant to Section 23 of the Personal Data Protection Act 2010)

Developed by
ASSOCIATION OF PRIVATE HOSPITALS OF MALAYSIA AS DATA USER FORUM FOR PRIVATE HOSPITALS

Contents

		Page no.
CODE OF PRACTICE FOR PRIVATE HOSPITALS		
1.	Introduction	3
2.	Status and Applicability	3
3.	Definitions	4
4.	Application of the Data Protection Principles in a Private Hospital Environment	6
	Illustration on the data flow in a Private Hospital from the initial collection of PD of the DS until the PD is destroyed.	6
5.	Rights of Data Subjects	19
6.	Specific Issues	24
7.	Employees	26
8.	Other Compliance Issues	27
9.	Code Review	28
10.	Conclusion	28

1. INTRODUCTION

1.1 This Code is developed by the Association of Private Hospitals of Malaysia ("APHM") pursuant to Section 23(1)(a) of the Personal Data Protection Act 2010 ("PDPA"). APHM was designated as the Data User Forum for Private Hospitals by the Personal Data Protection Commissioner ("PDPC") pursuant to Section 21 of the PDPA.

1.2 This Code is developed together with the assistance of the Personal Data Protection Commissioner.

1.3 This Code applies to all private healthcare facilities who are **licensed** as **Private Hospitals** under the *Private Healthcare Facilities & Services Act 1998*, (**"PHFSA" (Act 586)**) who will be considered as "Data Users" ("DU") for the purposes of the PDPA.

1.4 **Scope of the Code**
This Code aims to address compliance to the Data Protection Principles as set out in PDPA in the unique circumstances faced by Private Hospitals. Since the PDPA only provides "Principles" for compliance, this Code aims to provide some definitive guide to compliance to the stated principles insofar as it applies to Private Hospitals.

2. STATUS AND APPLICABILITY

2.1 This Code regulates the Processing of Personal Data ("PD") and Sensitive Personal Data ("SPD") of the Data Subjects ("DS") in a Private Hospital environment.

2.2 The Code also aims to ensure that rights of the DS with respect to their PD are balanced with the needs of the Private Hospitals to process their PD to provide medical services and related services to the DS.

2.3 **"Data Subjects"** or Stakeholders under this Code will comprise:

a. Patients who are seeking medical treatment at the Private Hospitals;
b. Hospital employees (nurses, doctors and support staff);
c. Medical Specialists or Medical Consultants);
d. Service providers for Private Hospitals (including contractors, vendors etc.);
e. Relevant Persons (Next of Kin, Guardians etc. as defined in PDPA)
f. Casual visitors to the Private Hospital;

2.4 **Compliance Requirements**

2.4.1 This Code is not intended to replace the PDPA. All the provisions of the PDPA will continue to apply to Private Hospitals (as DU) save where they are modified, enhanced or substituted by the provisions of this Code.

2.4.2 A DS is not considered to have breached this Code or the PDPA if they are mandated to comply with other applicable laws affecting general healthcare and in particular, Private Hospitals.

2.4.3 A DS shall also comply with any **PDPA Standards** that may be issued by the PDP Commissioner from time to time regulating the various Principles of the PDPA.

2.5 This Code will come into force upon registration by the PDP Commissioner.

2.6 This Code has been drafted in the English Language. In case of discrepancies between the English text version of this Code and the Bahasa Malaysia version (or any other translated version), the English version shall prevail.

2.7 For the avoidance of doubt, in the event of a conflict between:

(a) This Code;
(b) PDPA Standards issued by the PDP Commissioner;
(c) The provisions of the PDPA;
(d) Malaysian Medical Council (MMC) Guidelines and Codes;
(e) Any other Standards issued by the Ministry of Health or any other relevant government agency;
(f) Any other specific legislation affecting any of the PDPA Principles; that has a direct impact on the processing of PD by the DU, then the instrument or document setting the higher standard for compliance will prevail.

2.8 Illustrations and examples in this Code are meant to be guidance only.

2.9 The list of permitted disclosures to 3rd parties as set out in Appendix A is not intended to be exhaustive and the DU is expected to comply with this Code and the Disclosure Principle (Section 8 PDPA) at all times.

3. DEFINITIONS

In this Code, unless the context otherwise requires, defined words shall have the following meanings:

Words	Meaning
Collect	in relation to PD, means an act by which such PD enters into the control of the DU either at time of the first visit or at each subsequent visit by the DS to the Private Hospital
Disclose	in relation to PD, means an act by which such PD is made available by a DU to a third party as part of the Medical Purpose in treating the DS.
Data	Processor (DP) in relation to PD, means any person or entity, other than an employee of the DP, who processes the PD solely on behalf of the DU, and does not process the PD for his own purposes. For example, private third party laboratories, data centres, cloud service and storage providers who provide the DU with services

Data User (DU)	means the Private Hospitals who process PD or has control over or authorizes the processing of any PD but does not include a DP; In this Code, "Data User" and "Private Hospital" is used interchangeably
Data Subject (DS)	means an individual who is the subject of the PD and for the purposes of this Code refers to patients, employees etc. whose PD is processed as part of the Medical Purpose and related purposes.
Explicit Consent	means any freely given, specific, informed and unambiguous indication of the DS's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Healthcare Services	has the meaning assigned to it in the Private Healthcare Facilities and Services Act 1998 [Act 586]
Healthcare Professional	means a medical practitioner, dental practitioner, pharmacist, clinical psychologist, nurse, midwife, medical assistant, physiotherapist, occupational therapist and other allied healthcare professionals and any other person involved in the giving of medical, health, dental, pharmaceutical and any other Healthcare Services under the jurisdiction of the Ministry of Health who are employees or under contract of service with the Private Hospital.
Informed Consent	The process and the form by which a patient/DS learns from the Healthcare Professional or Medical Specialists about and understands the purpose, benefits, and potential risks of a medical or surgical intervention, including clinical trials, and then agrees to receive the treatment or participate in the trial.
Medical Devices	Shall have the same meaning ascribed to it under Medical Devices Act 2012.
Medical Purpose(s)	includes the purposes of preventive medicine, medical diagnosis, medical research, rehabilitation and the provision of care and treatment and the management of healthcare services (in other words encompasses end-to-end processing of the PD of the DS as part of the medical treatment provided to the DS)
Medical Specialists or Consultant	medical practitioner or dental practitioner under contract for service with the Private Hospital
Next of Kin	Means a person's closest living relative, including spouse children, parents and in some cases siblings
Private Hospital	means private hospitals and medical centres that are licenced under the PHFSA (Act 586).
Processing	in relation to PD, means collecting, recording, holding, use, disclosure and storing of the PD including, (a) the organization, adaptation or alteration of PD; (b) the retrieval, consultation or use of PD; (c) the disclosure of PD by transmission, transfer, dissemination or otherwise making available; or (d) the alignment, combination, correction, erasure or destruction of PD.

Relevant Person	in relation to a DS, howsoever described, means, (a) in the case of a DS who is below the age of eighteen years, the parent, guardian or person who has parental responsibility for the data subject; (b) in the case of a DS who is incapable of managing his own affairs, a person who is appointed by a court to manage those affairs, or a person authorized in writing by the DS to act on behalf of the DS.
Requestor	in relation to a data access request or data correction request, means the DS or the Relevant Person on behalf of the DS, who has made the request
Sensitive Personal Data or SPD	means any PD consisting of information as to, (a) the physical or mental health or condition of a DS, (b) his political opinions, (c) his religious beliefs or other beliefs of a similar nature, (d) the commission or alleged commission by him of any offence
Third Party	in relation to PD processed by the Private Hospital means any person or entity that is outside the purview or control of the Private Hospital who may be providing services to the Private Hospital.
Use	Means in relation to PD in a Private Hospital means the use of such PD for all Medical Purposes
Vital Interests	means matters relating to life, death or security of a DS.

4. APPLICATION OF THE DATA PROTECTION PRINCIPLES IN A PRIVATE HOSPITAL ENVIRONMENT

The following illustration shows the data flow in a Private Hospital from the initial collection of PD of the DS until the PD is destroyed.

4.1 Data Protection Principles

The PDPA provides that the processing of PD by a DU shall comply with the following Personal Data Protection Principles. The application of this Principles will be applied throughout the data flow as shown above. :

(a) the General Principle (which deals with consent);
(b) the Notice and Choice Principle;
(c) the Disclosure Principle;
(d) the Security Principle;
(e) the Retention Principle;
(f) the Data Integrity Principle; and
(g) the Access Principle

It should be noted that these are mere principles and the nature and method of compliance to the processing of PD in particular industries is left to the DU. **Hence, the purpose of this Code is to set out those unique compliance practices specific to Private Hospitals.**

4.2 General Principle – Consent (Section 6 PDPA)

4.2.1 Under the General Principle, consent must be obtained from the DS for the Processing of PD in a Private Hospital environment unless the Processing involves one of the scenarios stated in Section 6(2) of the PDPA, for which no consent is required.

4.2.2 For Sensitive Personal data (SPD), the DU must obtain **"Explicit Consent"** of the DS. **SPD** as defined in the PDPA means:

(a) the physical or mental health or condition of a DS;
(b) political opinions of a DS;
(c) religious beliefs or other beliefs of a similar nature of a DS;
(d) the alleged commission of any offence by a DS.

4.2.3 DU shall not process PD unless,

(a) the PD is processed for a lawful purpose directly related to an activity of the DU.
(b) the processing of the PD is necessary for or directly related to that purpose; and
(c) the PD is adequate but not excessive in relation to that purpose

In this regard, the DU must ensure that all Private Hospital Forms are reviewed to remove the collection any excessive personal information that is not required for Medical Purposes and other related purposes.

4.2.4 PD collected from DS (Patients, Employees and others) includes but limited to:

(a) Name
(b) Address
(c) NRIC Number/Passport Number
(d) Date of Birth
(e) Place of Birth
(f) Sex
(g) Race
(h) Religion
(i) Occupation
(j) Marital Status
(k) Nationality
(l) Telephone number
(m) Email address
(n) Next of Kin's/Guardian's personal details ("Relevant Person")

(o) Credit Card Details
(p) Educational Qualifications (for employees)
(q) Professional Qualifications of Medical Personnel and Specialists
(r) Medical history and other relevant information
(s) Biometric information (such as fingerprints)
(t) DNA profiles
(u) Photographs and Videos
(v) Family physician's particulars
(w) And other information that may be used to identify the DS and required to provide healthcare services by the DU.

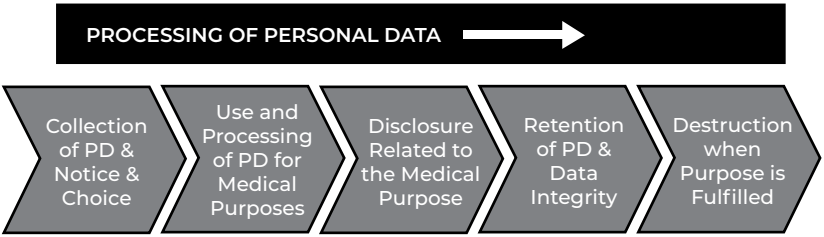
4.2.5 In situations where a DS voluntarily provides his PD to the DU for a stated purpose, which under this Code will be for Medical Purpose, it will constitute Explicit Consent to the Processing of his PD for Medical Purpose and related medical purposes.

4.2.6 In situations where the DS is incapable of giving consent (for example he is incapacitated or injured) at the time of admission, the consent may be procured soon thereafter or from the Relevant Person.

4.2.7 In cases of a minor (i.e a person who is under the age of eighteen) or where the DS is incapable of giving Consent, then such Consent may be given by the "Relevant Person".

4.2.8 In the case of PD of Relevant Person and other relevant parties to be contacted in case of emergency (where the DS is incapacitated or unable to give consent), the Private Hospitals will assume that the DS has procured their Consent for the Private Hospitals to process their PD for the purpose of being contacted.

4.2.9 In the case of Private Hospital processing patient data, such Consent will be considered as given for "Medical Purpose". By way illustration the data flow in a Private Hospital can be represented in the following diagram:



4.2.10 Any collection and processing of PD from patients for non-medical purposes will require additional consent to be obtained. This type of consent will be required for activities such as use of PD for medical research, medical trials and marketing activities of the DU, which is unrelated to the Medical Purpose.

4.2.11 The PDP Regulations provides that "consent" must be obtained by any method capable of being recorded and maintained by the DU such as:

(a) Signing a registration form
(b) Clicking a box in a form signifying consent (Opt-in)
(c) Implied consent (eg. consent given through an authorised person, or)
(d) By conduct or performance (eg. via phone)
(e) Any other written documentation

4.2.12 Private Hospitals should always obtain consent from DS by an **"Opt-in"** method as opposed to an **"Opt-out"** method. (For example: In any hospital forms, asking a DS to tick a box saying: "tick the box if you do NOT wish to receive promotional material").

4.2.13 PD is collected by DU through the following channels in a Private Hospital environment: but not limited to

(a) Patient registration forms (out-patient or in-patient);
(b) Employment application forms (for staff, nurses, doctors etc.);
(c) From any third parties connected with the patient such as the parent gu ardian, employer/potential employer, agents (e.g. medical tourism agents), insurance companies, other healthcare facilities
(d) Specific medical procedures forms (surgery and other procedures) which may include Informed Consent Form;
(e) Feedback Survey forms;
(f) Information update forms;
(g) Clinical Research Application Forms;
(h) Medical Specialists agreements with the DU;
(i) Access Request forms;
(j) Images recorded through CCTV or other electronic media;
(k) Other information or documents provided by a Data Subject in writing, over the telephone, electronically by Email or through the DU's corporate website; and
(l) PD obtained as part of the DU's role as Data Processor for third parties (where the DU provides teleradiology services, lab services etc.)

4.2.14 The following examples are situations covering **Medical Purposes** where consent may be given explicitly or where exceptions to the consent obligation may apply:

(a) By the DS voluntarily provides his PD by filling up patient registration forms, feedback forms, information update forms and such like communication with the Private Hospital, it will be considered that the DS has given his "explicit consent" to the Processing of his PD for the purposes of getting medical treatment at the Private Hospital.

(b) The medical treatment process where PD will be collected and processed may encompass the following activities:

(i) examination by a Medical Specialist or a Healthcare Professional consultant;
(ii) provision of treatment as out-patient or in-patient;
(iii) undergoing diagnostics tests such as x-rays, CT scans, ultrasound, lab tests etc.;
(iv) undergoing surgical procedures (where DU obtains a further Informed Consent for the surgery);
(v) case conference between other Medical Specialists or Healthcare Professionals within the Private Hospital or from other hospitals;
(vi) procurement of insurance, dealings with managed care organisations, employers or third party guarantors to cover cost of treatment;
(vii) dealing with debt recovery agents and lawyers to recover costs of healthcare services provided to the DS;
(viii) follow-up consultations; and
(ix) all other sharing of PD relating to medical treatment of a DS.

4.3 Notice and Choice Principle (Section 7 PDPA)

4.3.1 The PDPA requires DU to notify the DS of the purpose for the collection, use and disclosure of PD of the individual and obtain his/her consent which must be recorded and maintained, unless any relevant exception in Section 6 (2) of the PDPA applies.

4.3.2 The DU must inform, disclose or display their PDP Notice to the DS at the time of collection or as soon as practicable thereafter.

4.3.3 The PDP Notice must contain the following information:

(a) that PD of the DS is being processed by or on behalf of the DU and provide a description of the PD:

Example:
That the PD is processed by the Private Hospital or authorised Data Processor on behalf of the Private Hospital such as the medical Specialists, Outside Labs etc.

(b) the purposes for which the PD is being or is to be collected and further processed with the consent of the DS. This will include both Medical Purposes and related purposes;

Examples Include:

- PD collected and processed for Medical Purpose and related healthcare services
- To establish and manage medical records and medical reports
- To facilitate payment process relating to the patients
- To institute debt recovery proceedings against defaulters
- To report the personal data to the relevant authorities and/ or third parties under the governing laws relevant to the healthcare industry
- To share the personal data with group holding company and related companies (where required) as defined in the Companies Act 2016
- To conduct research, analysis and improvement
- To market and advertise products and services
- To facilitate overseas patients personal requirements (for example visa applications)
- To administer and respond to request, queries, complaints and legal issues
- To facilitate human resource management activities relating to employees
- For submission and registration of relevant forms, licenses to the relevant regulatory authorities and/or third parties under any governing laws relevant to the healthcare industries
- To share personal data for the purpose of banking facilities, legal advice and audit
- For education and training (with anonymised PD wherever possible)
- For any other purpose that is incidental or in furtherance to the above purposes

(c) any information available to the DU as to the source of that PD;
(d) DS's right to request access to and to request correction of the PD;
(e) The contact details of the Compliance Officer or the Data Protection Officer of the Private Hospital for any inquiries or complaints in respect of the PD;
(f) of the class of Third Parties to whom the DU discloses or may disclose the PD, (for example third party vendors who provide services to the DU in the course of providing Medical Services, such as outside labs, insurance companies etc.;
(g) of the choices and means the DU offers the DS for limiting the processing of PD, including PD relating to other persons who may be identified from that PD;
(h) whether it is obligatory or voluntary for the DS to supply the PD;
(i) where it is obligatory for the DS to supply the PD, the consequences for the DS if he fails to supply the PD.

4.3.4 When to give Notice. The PDP Notice shall be given as soon as practicable by the DU:

(a) when the DS is first asked by the DU to provide his PD;
(b) when the DU first collects the PD of the DS as set out paragraph 3.2.14;
(c) or in any other case, before the DU, (i) uses the PD of the DS for a purpose other than the purpose for which the PD was collected; or (ii) discloses the PD to a third party.

4.3.5 Method of communicating PDP Notice. The PDP Notice to the DS may be communicated by one or more of the following ways:

(a) By delivering a printed copy of the summary of the notice to the DS at the time of first registration as a patient or when joining as an employee or as a specialist in the Private Hospital or soon thereafter;
(b) By posting a summary of the notice at key places in the Private Hospital (for example on electronic boards and posters);
(c) By verbally explaining to the DS prior to collecting PD throughout the treatment process in the Private Hospital;
(d) By verbally explaining to the DS prior to carrying out special medical procedures where explicit consent is required (example for operations and other procedures not covered by the general consent).
(e) By directing the DS to the DU's Website.

4.3.6 The PDP Notice shall be in Bahasa Malaysia and English languages.

4.4 Disclosure Principle (Section 8 of the PDPA)

4.4.1 The disclosure of the DS's PD is limited to the purpose and related purposes for which the original consent was obtained under the Notice and Choice Principle.

4.4.2 No PD shall be disclosed for any purpose other than:
(a) The purpose for which the PD was to be disclosed at the time of collection, which in the case of Private Hospitals shall be all activities related to the Medical Purpose; or

Example: This will include all activities relating the provision of medical treatment, including examination, consultation, diagnostics, lab tests, treatment, surgeries, processing payment etc.

(b) a purpose directly related to the original purpose;
(c) to any party other than a third party of the class of third parties as specified in **Appendix B**. This list shall be updated on periodical basis by the DU.

4.4.3 Extent of further disclosure of PD which falls outside the consent given by the DS for the original purpose at the time collection. Such disclosure may be made under the following circumstances:

(a) The DS has given his consent for the disclosure;
(b) For the purpose of detecting a crime or for the purposes of investigations:

Example 1 : To detect theft of hospital equipment or supplies, the DU discloses employee's or patient's PD to investigators or to the Police

(c) Was required or authorised by or under any law:

> Example : Where the Hospitals are required to disclose information to the Ministry of Health in cases of notifiable diseases.

(d) The DU acted in the reasonable belief that it had in law the right to disclose the PD to the other person:
(e) The DU acted in the reasonable belief that it would have had the consent of the DS, if the DS had known the circumstances of such disclosure:
(f) The disclosure is justified as being in the public interest as determined by the Minister;
(g) Permitted disclosure where required by a government agency, statutory requirement or a court order.

4.5 Security Principle (Section 9 of PDPA)

4.5.1 Under the Security Principle, the DU, when processing PD, is required to take ***'practical steps'*** to protect PD from loss, misuse, modification, unauthorised or accidental access or disclosure, alteration or destruction.

4.5.2 ***'Practical Steps'*** is not defined in the PDPA but the DU should incorporate adequate physical and electronic measures to protect the PD. The threshold required for PD processed in a Private Hospital environment is high since a large part of the processing involve Sensitive Personal Data.

4.5.3 The physical and electronic measures that the DU needs to take must have regard to:

(a) The place or location where PD is stored:

> This is critical in particular if the PD is being stored outside the Hospital premises, such as a Cloud Storage, then secure encrypted communication protocols must be implemented when transmitting and retrieving PD from such location.

(b) Security measures incorporated into any equipment in which PD is stored:

> 1. The entire IT System in a Hospital has to be secure with adequate firewalls, anti-virus and other anti-intrusion software.
> 2. Particular attention must be paid to Diagnostic equipment such as CT Scan, Ultrasound, X-ray, storage servers etc, that holds patient data to ensure that they have adequate safeguards from unintended disclosure or unauthorised access.
> 3. Again, particular attention should be had to the giving of remote access to vendors and other third party service providers to hospital IT Systems (especially the Diagnostic equipment).

(c) Measures taken to ensure reliability, integrity and competence of personnel of the Private Hospital having access to the PD:

1. The Hospital has to ensure that all hospital staff are adequately trained in protecting the security and integrity of PD.

2. All personnel having access to IT systems must be educated in the importance of keeping PD secure. The Hospital shall ensure that access protocols are tightly controlled on a need to know basis.

(d) Measures taken for ensuring the secure transfer of PD:

1. Physical movement of Medical Records within the Hospital environment should be under secure conditions. For example, the MR should be transported in dark covered pouches when they are moved from the Medical Records Room to the individual clinics.

2. If the PD is stored in the cloud, then the choice of the cloud service provider and communication protocols must be secure

4.5.4 Other Security Measures that DU should take to secure PD. These are only minimum standards and the DU shall be at liberty to incorporate enhanced measures to secure PD that it processes

(a) Administrative Processes enforced via PDPA Policies:
- (i) Regular and continuous training on data protection for all employees, Healthcare Professionals and where relevant for Medical Specialists;
- (ii) How PD is to be handled in the various departments of the Private Hospital and in particular at the Specialists Clinics;
- (iii) Physical movement of PD within and outside the Private Hospital (should include movement of Medical Records from the Medical Record's Room and around the Private Hospital);
- (iv) Access protocol setting out who gets access to PD of patient/ DS across the whole Private Hospital;
- (v) Access to patients'/ DS's PD by Medical Specialists who have multiple clinics in different hospitals;
- (vi) Strong policies on the use of portable storage devices such as USB-drives. If required, has to be approved by the Chief Information Officer of the Private Hospital ("CIO") or any authorized personnel of the Private Hospital.

(b) Electronic measures to protect PD:
- (i) All communication containing PD must be encrypted;
- (ii) Installing adequate firewalls, anti-intrusion software and up-to-date virus definitions;
- (iii) All electronic devices must be password protected (e.g. Laptops, diagnostic devices, i-pads etc;

(iv) Access control to Hospital Information Systems (HIS) with audit trail;
(v) Complete back-up of all PD processed by the Private Hospital in a remote site away from the hospital premises;
(vi) Disaster recovery and business continuity policies must be in place;
(vii) Limit use of portable storage devices to transfer PD and only if authorised by CIO or other top management

(c) Physical measures
(i) Door access to rooms where PD is kept is to be strictly controlled;
(ii) Physical Medical Records to be kept in secure room with access limited to only employees managing the Medical Records;
(iii) Movement of Medical Records must be in closed bags or boxes;
(iv) All medical files, records and other information should be kept out of sight of other patients and third parties when they are at the nurses' station;
(v) Set up a Data backup system of all HIS data in a location outside the Private Hospital to serve as a disaster recovery mechanism;
(vi) Install CCTVs in strategic areas of the Private Hospital to deter theft of PD.

(d) Additional measures that should be taken by the DU to ensure security include:
(i) physical security measures to prevent unauthorized access;
(ii) access and authorization processes to ensure only legitimate users have access to the medical record and that each user has the appropriate level of access to the medical records;
(iii) the maintenance of audit logs to support the authenticity of additions to the Medical Records;
(iv) the protection of any part of an electronic Medical Record from being deleted;
(v) read-only formats for external documents stored in the Medical Records;
(vi) adequate protection whenever Medical Records are disclosed to health care providers or patients;
(vii) regular back-up of the Medical Records, preferably daily for in-patients;
(viii) adequate virus protection to ensure the Medical Records are not modified or destroyed by external factors;
(ix) contingency plans for disaster recovery and denial of service attacks;
(x) ensure that no hardware contains any personally identifiable patient information prior to disposal which must be complete;
(xi) enhanced security e.g. additional encryption or authentication processes, when networks are more exposed e.g. wireless devices and remote access, or where the equipment that store information are on drives that are at risk of loss or theft e.g. laptops, USB drives, tablets and I-Pads etc.

4.5.5 Data Processors ("DP")

Where PD is processed by a DP on behalf of the DU, the DU shall ensure that, (i) the DP provides sufficient guarantees in respect of the technical and organisational security measures governing the processing and (ii) takes reasonable steps to ensure compliance with those measures.

Examples of Data Processors:
a. Medical Specialists in the Hospital;
b. Outsourced Data Centres;
c. Outside Labs providing diagnostic services;
d. Outsourced Human Resource services.

Some prudent steps that the DU can take prior to employing a DP include:

(a) Ensuring that a **pre-agreement** vetting of the DP is undertaken to ensure the following:
   (i) The DP has adequate policies and procedures to keep the DU's PD securely;
   (ii) Has stringent access controls to the PD of the DU by only allowing access on a need-to-know basis;
   (iii) The DP's premises are secure from any cyber threats;
   (iv) Has a back-up protocol to ensure business continuity for the DU is maintained;
   (v) That they have incorporated into their facility all prudent technical and electronic safeguards to protect the PD entrusted to them;
   (vi) They have adequate safeguards, particularly in respect of use, security, retention and destruction of PD.

(b) Upon being satisfied that the DP has complied with (a) above, the DU should enter into a **formal agreement** with the DP which covers the following issues:

   (i) robust non-disclosure provisions;
   (ii) undertaking that their facility has current anti-virus, firewall and up to date anti-intrusion software;
   (iii) right to regularly audit their security systems;
   (iv) right to inspect their policies relating to storing and processing PD including access rights to their employees;
   (v) incorporating encryption in all transmission and reception of PD;
   (vi) back-up and restore functions and a clear protocol to maintain business continuity;
   (vii) Right to claim compensation for loss of the PD in their custody;
   (viii) Obligation to report a data breach at the DP's data facility to the DU within one (1) hour of becoming aware of a breach;

4.6 Retention Principle (Section 10 of the PDPA)

4.6.1 The PDPA states that the PD processed for any purpose shall not be kept longer than is necessary for the fulfilment of that purpose.

4.6.2 This retention principle does not prescribe any particular period of retention but for Private Hospitals it will be governed by Healthcare Industry standards, PHFSA (Act 586) and other related legislation including industry practice as stated in Clause 3.6.5 below.

4.6.3 Under the Limitation Act 1953, actions founded on a contract (amongst others) must be brought within 6 years from the date on which the cause of action accrued. Hence the DU may wish to retain records relating to its contracts for 7 years from the date of termination of the contract and possibly for a longer period if an investigation or legal proceedings should commence within that period.

4.6.4 The provisions of other specific legislation concerning retention of PD will not be affected by the retention principle of the PDPA. Retention periods provided by these Acts including: Financial Services Act 2013, Limitation Act 1953, Income Tax Act 1967 etc. should be complied with by the DU;

4.6.5 Typical Retention periods for Private Hospitals are as set out in the Table below. However, this may vary depending on the dictates of specific legislation, industry practice or other regulatory requirements. :

No.	Types of Use of Personal Data	Retention Period
1.	Personal Data of Patients	7 years for adults and 25 years for newborns calculated from their last visit date
2.	Employee PD	For the duration of employment and 7 years thereafter
3.	Visitor PD	No longer than 3 months
4.	CCTV Data	30-60 days unless required as evidence of a criminal investigation
5.	Legal Proceedings (Civil or criminal)	Until conclusion of investigation and trial and any Appeals thereafter
6.	Retention required by Law	Retaining PD beyond the relevant periods required by law is permissible
7.	Retention on Electronic Media or servers	Retaining PD beyond the prescribed period may be possible if security of the PD can be maintained throughout the period. However, the DU must be mindful if using old PD as it may not be up-to-date or accurate for further processing
8.	Retention of physical Forms containing PD after they have been digitised and converted into an electronic format	Retention of hard copies should be for a maximum period of 30 days unless required for legal, tax and other statutory purposes. In the event hard copies are retained, their security must be safeguarded.

9	Anonymised Personal Data	These types of PD may be kept without restriction so long as it is Not identifiable as PD

4.6.6 Destruction of Personal Data. The general principle is that the DU must take reasonable steps to ensure PD is destroyed or permanently deleted if no longer required for the purpose it was collected. Private Hospitals should adhere to the guidelines issued by MOH – "Jadual Pelupusan Rekod Perubatan 2016".

4.6.7 ***Destruction*** will apply to hard copies of documents that contains PD. In case of Private Hospitals, it will refer to the various forms used around the Hospital. (eg. Registration, medical procedures, visitor logs and other transient collection of PD such as CVs of employees). Once the PD obtained via these forms has been transferred to a data server and kept in an electronic format, they may be considered for destruction unless hard copies are required to be retained for specific purposes as stated earlier.

4.6.8 ***Permanent deletion*** will apply to PD contained in electronic medium (such as hard drives and USB drives, Laptops, X-ray machines, CT Scan machines etc.).

4.6.9 Destruction of PD and SPD obtained and processed in a Private Hospital environment needs special methods of destruction or deletion which includes:

(a) Incineration of documents and electronic media (both PD and SPD)
(b) Shredding of paper documents that contain ordinary and transient PD;
(c) Hiring specialist firms to shred documents that contain PD/SPD at the Private Hospital premises and not removed elsewhere
(d) PD contained in electronic media should be deleted using the latest technology such as magnetic degaussing;
(e) Old hard-drives from personal computers should be physically destroyed or crushed.

4.6.10 Anonymisation of Personal Data
The Private Hospital as a DU will be considered to have ceased to retain PD when it no longer has the means to associate the PD with particular DS – i.e. the PD has been anonymised. Anonymisation of PD is a recommended method when data is required for research, education or for uses that does not require identifiable information.

4.7 Data Integrity Principle (Section 11 of the PDPA)

4.7.1 A DU shall take reasonable steps to ensure that the PD is accurate, complete, not misleading and kept up-to-date by having regard to the purpose, including any directly related purpose, for which the PD was collected and further processed.

4.7.2 The following would amount to reasonable steps in a Private Hospital environment to ensure that the PD is accurate, complete, not misleading and kept up-to-date.

(a) Allowing the DS themselves to fill up application and other forms;
(b) Collecting PD through Electronic upload (such as NRIC);
(c) Having a procedure to encourage DS to update their PD if there are changes, for example their marriage status, address, change of religion etc;
(d) Ensuring that PD is updated each time the DS visits the Private Hospital.

4.7.3 The Data Integrity principle does not require the DU to verify or guarantee the accuracy or completeness of the PD but only take reasonable steps.

4.7.4 In cases where it involves a Minor or DS who are incapacitated, the DU may rely on family members or relatives to provide the PD of the patient/ DS and to update such information as required.

4.8 Access Principle (Section 12 & Section 30 of the PDPA)

4.8.1 DS's has a right to request access to and to request correction of his PD. In that regard, the DU shall make available an Access Request Form in a physical form or online (a sample Access Request Form is attached as Appendix B).

Under the Access Principle, the DU is required to :

(a) give access to the PD of the DS held by the DU upon a request and payment of the prescribed fee or any fees permitted by the Commissioner.; and
(b) the right to correct that PD where the PD is inaccurate, incomplete, misleading or not up-to-date
(c) Prescribed Fee for Access Request

Hospitals receiving a Data Access Request may charge a fee for each Data Access Request. The maximum fees that can be charged, as provided by Personal Data Protection (Fees) Regulations 2013 as set out below:

Item	Description	Maximum Fee (RM)
1	Data Access Request for a DS's PD with a copy	10
2	Data Access Request for a DS's PD without a copy	2
3	Data Access Request for a DS's Sensitive PD with a copy	30
4	Data Access Request for a DS's Sensitive PD without a copy	5

4.8.2 All DU should ensure that this right to Access is clearly set out in the Privacy Policy and also make available an Access Request Form on-line.

5. RIGHTS OF DATA SUBJECTS

5.1 Rights of Access to Personal Data by a Requestor (Section 30 of PDPA)

A Requestor may make a data access request in writing to the DU upon payment of prescribed fee for information of a DS's PD that is being processed by or on behalf of the DU; provided that the Requestor:

a. have furnished the DU or DP (whichever is applicable) the consent form of the DS authorizing and indemnifying the DU or DP to release/ or correct the PD of the DS; and

b. shall communicate to the DS a copy of the said DS's PD in an intelligible form upon receiving the same from DU or DP (whichever is applicable).

5.2 Rights of Access to Medical Records[1]

5.2.1 A medical record is documented information about the health of the DS recorded by a Healthcare Professional, either personally or at his or her instructions. It contains sufficient information to identify the DS/ patient, support the diagnosis based on history, physical examination and investigations, justify the professional management given, record the course and results thereof, and ensure the continuity of care provided by the attending Healthcare Professional to that particular DS.

5.2.2 Medical records are aide memoirs for Healthcare Professional treating patients and as essential components to patient care. They contain information about the patient, on one part, and the physician's opinion and clinical judgment which brought to bear on the patient's management, on the other part. Based on these concepts, the Medical Records were considered "confidential" documents and the information therein contained considered "private" in observance of ethical doctor- patient relationship.

5.2.3 It is well established that Medical Records are the property of the DU/ Private Hospital, but the DS has a right of access to the information contained in those records. The personal information (name, address, identification data, etc.) that the Healthcare Professional has recorded belongs to the patient.

The DS may seek access for various purposes, ranging from a need to seek second opinion from another hospital or practitioner, to seek further treatment elsewhere, or for litigation purposes. This right of access is also extended with the DS's consent, to the DS's appointed agents, guardians or Relevant Persons.

5.2.4 Contents of a DS/Patient's Medical Record

The following intellectual and physical items may, in whole or in part, make up the contents of a DS/Patient's Medical Record:

(i) Patient's personal information (obtained as discussed earlier)
(ii) Doctor's clinical notes (contemporaneous notes written at the time of seeing the patient or thereafter)
(iii) Recording of Discussion with patient/Relevant Persons regarding disease/ management (with witness) / Possible use of tape recording for such discussions
(iv) Referral Notes to other specialist(s) for consultation/co-management

[1] *MMC Guideline on Medical Records & Medical Reports*

(v) Laboratory & Histopathological reports
(vi) Imaging records and reports
(vii) Clinical Photographs
(viii) Drug Prescriptions
(ix) Nurses' Reports
(x) Consent Forms, At-Own-Risk Discharge Forms
(xi) Operation Notes/Anaesthetic Notes
(xii) Video Recordings
(xiii) Printouts from monitoring equipment (e.g. Electro-cardiogram, Electro- encephalogram)
(xiv) Letters to and from other health professionals
(xv) Recordings of telephone consultations/instructions relevant to the care of the patient

5.2.5 Access to Medical Records

The PDPA prescribes that the DS should have access to his PD that is contained in the Medical Records maintained by the DU. This right is also set out in the MMC Guidelines as follows, that the DS/patient shall:

(a) have access to records containing information about his/her medical condition for legitimate purpose and in good faith;
(b) know what personal information is recorded and processed;
(c) expect the records to be accurate, and
(d) know who has access to his/her personal information.

While patients have right of access to their Medical Records, they also have a right to inform the attending Healthcare Professional or authorised personnel of the Private Hospital of any factual errors in the personal information contained in the Medical Records and have it corrected. Patient/ DS are not allowed to change any entries made by the attending Healthcare Professional in the course of consultation, diagnosis and management as these are made by the practitioner based on his clinical judgement.

PD of other individuals. The DS do not have access to any information or identity of another individual contained in the Medical Record. If the identity of is already known to the DS, then the data containing the information relating to the third party can be revealed to the DS.

The DU has to consider whether it is possible to separate the PD of any other individuals from the other information of the DS that will be disclosed, for example, by blanking out the name of the individual, or blanking out other identifying particulars would be sufficient to disguise the identity of the individual from the D S.

Copy of the Medical Records only be taken out of the Hospital custody in limited circumstances, either by a court order, or mutual consent of the DU and the DS. In all cases where the original Medical Record is taken out due to Court Order, a copy of the records shall be retained at the Hospital.

5.2.6 Medical Reports

Medical Reports are documents prepared by an attending doctor on a patient/DS based on his Medical Record. Opinion by an expert may also be part of a Medical Report.

The DU shall provide comprehensive Medical Reports when requested by the DS or by the Next of Kin in the case of children or minors, or by the employer with the DS's/patient's specific and explicit consent within the time stipulated in the PDPA.

5.2.7 Denial of Disclosure of Medical Records

The DU may deny access to the contents of the Medical Record, if in their considered opinion:

(a) the DU is not supplied with sufficient information to satisfy himself as to the identity of the Requestor;
(b) the contents if released may be detrimental or disparaging to the DS, or any other individual, or
(c) liable to cause serious harm to the patient's/ DS's mental or physical health or endanger his life.
(d) if there is no written consent from the patient, or his legal next-of-kin or guardian, for release of the contents of the Medical Record to a third party;
(e) the patient/DS is deceased, and a request is received from someone other than the next-of-kin.
(f) and all other scenarios mentioned in Section 32 of the PDPA.

5.2.8 The current prescribed fee for access to PD by a DS is regulated by the PDP Commissioner in the PDP (Fees) Regulations 2013 (See Para 3.8.1.(c) . The DS may request to have sight of the documents in the Medical Record or ask for copies to be made of relevant parts of the MR.

5.2.9 The DU must comply with Access Request within 21 days but no later than 35 days from the date of receipt of the request, unless the DU is able to fall within any of the exceptions in Section 32. However, the DU needs to inform the requester in writing with reasons as to why he is unable to comply with the access request with the initial 21-day period.

5.2.10 The right to correct PD may be refused by the DU if the conditions under Section 36 of the PDPA are met by the DU.

5.3 Right of Data Subject to withdraw consent to process Personal Data (Section 38 of PDPA)

5.3.1 A DS may by notice in writing to the DU withdraw his consent to the processing of PD in respect of which he is the data subject.

5.3.2 The DU shall, upon receiving the notice cease the processing of the PD.

5.3.3 However, the right to withdraw consent shall not apply for on-going medical treatment and its related services, which requires the DU to continually process the PD of the patient/ DS in the course of giving medical treatment for the DS.

5.3.4 If for any reason, the DS decides to withdraw his consent given for Medical Purposes, it will mean that the DU will have to cease processing the PD of the particular DS and the DU cannot continue to provide treatment or other medical services to the DS who has withdrawn his consent.

5.3.5 The right to withdraw consent in a Private Hospital environment may apply to limited circumstances such as:

(a) Marketing of DU's other services unrelated to treatment;
(b) Participation by the DS in clinical trials (where PD is required to be processed);
(c) Exchange of Patient Data with other medical practitioners;
(d) Taking of pictures of DS (or any part of his body) whilst undergoing treatment or surgery; and
(e) Any other purpose not related to Medical Purpose.

5.4 Right to prevent processing likely to cause damage or distress (Section 42 of the PDPA)

5.4.1 A DS may, at any time by a giving "data subject notice" in writing to a DU, require the DU (a) cease the processing of or processing for a specified purpose or in a specified manner; or (b) not begin the processing of or processing for a specified purpose or in a specified manner, any PD in respect of which he is the data subject if, based on reasons to be stated by him:

(a) the processing of that PD or the processing of PD for that purpose is causing or is likely to cause substantial damage or substantial distress to him or to another person; and
(b) the damage or distress is or would be unwarranted.

5.4.2 The right in 4.3.1 shall not apply where:

(a) the DS has given his consent; or
(b) the processing of PD is necessary in order to protect the Vital Interests of the DS; and
(c) other reasons stated set out in Section 42 of the PDPA.

5.5 Right to prevent Processing for Direct Marketing (Section 43 of the PDPA)

5.5.1 A DS may, at any time by notice in writing to a DU, require the DU to cease or not to begin processing his PD for purposes of Direct Marketing. If the DU wants to send marketing materials to their patients, then it would be advisable to obtain express consent from the DS with information on how the marketing will be communicated.

5.5.2 "Direct Marketing" means the communication by whatever means of any advertising or marketing material for the DU's services which is directed to particular individuals. This will include letters, flyers, SMS, WhatsApp, Email etc.

6. SPECIFIC ISSUES

6.1 Sensitive Personal Data (SPD) (Section 40 of the PDPA)

6.1.1 The PDPA provides that a DU shall not process any SPD of a DS except in accordance with, inter alia, the following conditions:

(a) the DS has given his explicit consent to the processing of the SPD:

In most instances where the Hospital processes PD, it would have obtained the explicit consent of the DS by making the DS fill up the various forms prior to the processing the PD (as discussed earlier).

(b) the processing is necessary (where consent of PD is not necessary):
- (i) in order to protect the Vital Interests of the DS or another person, in a case where, (a) consent cannot be given by or on behalf of the DS; or (b) the DU cannot reasonably be expected to obtain the consent of the DS;
- (ii) for medical purposes and is undertaken by (a) a Healthcare Professional; or (b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a healthcare professional;

For example,
(a) where medical treatment is administered to accident victims using information from personal documents such as NRIC;
(b) to treat psychiatric patients who are incapable of giving consent

- (iii) for the purpose of, or in connection with obtaining legal advice for legal proceedings;
- (iv) for the purposes of establishing or defending legal rights;
- (vi) for the exercise of any functions conferred by or under any written law
- (vii) for the administration of justice;

For example,
(a) for investigation into a crime, where SPD is shared with the Police or other agencies;
(b) defending a claim brought against the DU or any Doctors in the Hospital, such as sharing SPD with Lawyers;
(c) sharing of SPD with Ministry of Health of information relating to communicable diseases (like AIDS), Dengue etc.

(c) the information contained in the PD has been made public as a result of steps deliberately taken by the data subject.

For example,
(a) where the DS gives an interview and the ensuing article is published in a newspaper or a magazine or containing the SPD of the DS
(b) The DS publishes his SPD in social media channels such as Facebook, Instagram, WeChat etc.

(d) All other instances as set out in Section 40 of the PDPA.

6.2 Medical Specialists employed under contract of service

6.2.1 If the Medical Specialists are employed under a contract of service, all obligations to PD accorded to employees will equally apply to these Medical Specialists.

6.3 Medical Specialists engaged under contract for service (as Consultants – also classified as "Data Processors")

6.3.1 The Medical Specialists have a special relationship with the Hospital and to their assigned patients in that, despite not being an employee, they have access to all the PD and SPD of such assigned patients within the custody of the Private Hospital as the DU. The Medical Specialists will be for all intents and purposes, considered a DP pursuant to Section 9 (2) of PDPA.

6.3.2 The Hospital must ensure that there are adequate contractual safeguards in the written agreement governing the relationship between the Private Hospital and the Medical Specialists that the Medical Specialists shall abide by the requirements of the PDPA to keep the PD of the patients/ DU in accordance with hospital policies, the Act, this Code and any applicable laws rules and regulations. Medical Specialists should be made aware of their role and responsibility towards PD of patients and the DU shall also ensure adequate training on the PDPA is provided to the Consultants.

6.3.3 This Code recognises the fact that Medical Specialists typically have clinics in multiple Private Hospitals hence, any access to or processing of PD of patient/ DS from one Private Hospital to another are not allowed unless it is consented by the patient/ DS.

6.3.4 DU shall have strong policies regulating the use of portable electronic devices by Medical Specialists unless they are fully encrypted and password protected.

6.4 Transfer of Data to Places Outside Malaysia

6.4.1 The PDPA prohibits the transfer of PD of a DS to a place outside Malaysia unless such place has been designated by the Minister as a safe place to process PD.

6.4.2 Notwithstanding the above, a DU may transfer PD to a place outside Malaysia if:
(a) The DS has given his consent.

This consent will be obtained from the outset at the time of first registration by a patient (by incorporating a consent in the registration form).

(b) The transfer is necessary for the performance of a contract between the DS and DU.

Example:
(a) transfer of a patient to an overseas branch or hospital for specialist medical treatment;
(b) sharing of PD where PD requests for 2nd opinion from an overseas consultant

(c) The transfer is for the purpose of legal proceedings or for the purpose of obtaining legal advice;
(d) The transfer is necessary to protect the Vital Interests of the DS;
(e) The transfer is necessary in the public interest as determined by the Minister.

7. EMPLOYEES

7.1 Applicability of PDPA to Employees

"Employees" will include Healthcare Professionals, hospital management personnel, general medical staff, administrative staff, IT personnel, security personnel etc., who are employed under a contract of employment with the Private Hospital.

7.1.1 The DU shall comply with all the Data Protection Principles of the PDPA when dealing with employee PD :

(a) The General Principle – Employee Consent should be obtained for all purposes connected with employment. For the PD of next of kin and emergency contacts, it will be considered to have been procured by the employee.
(b) Notice & Choice Principle – This will be complied by the DU upon the offer and acceptance of employment and the Employee signs the various Hospital policies and non-disclosure undertakings.
(c) Disclosure Principle – Disclosure of Employee PD will include any Third Party and unlimited to insurance companies, MCOs, Lawyers, Banks, travel companies and other employment related purposes.
(d) Security Principle – All PD will be kept reasonably secure from unauthorised access or disclosure or destruction.
(e) Retention Principle – Typically all Employee PD will be kept for 7 years after cessation of employment. All PD (in the form of CVs) supplied by potential candidates who are unsuccessful shall be destroyed within a reasonable time after the interview.
(f) Data Integrity Principle – All Employee PD processed by the DU shall be kept accurate and complete. Periodic exercise to update records should be initiated by HR policies and through Intra-net service where available.
(g) Access Principle – All Employees will be given access to their PD processed by the DU and a right to correct their PD where it is incomplete and not uptodate.

8. OTHER COMPLIANCE ISSUES

8.1 The Data User's compliance obligations in safeguarding Personal Data of Data Subjects shall be as follows:

(a) Comply with the all the provisions of the PDPA except where this Code provisions modify the obligations or rights of the DU or DS;
(b) Specific legislation affecting the healthcare industry and Private Hospitals in particular shall take precedence over the provisions of the PDPA or this Code.
(c) The DU should consider appointing a Data Protection Officer with powers to implement, manage and enforce the PDPA and the Code provisions at the respective Private Hospital.

8.2 Compliance Monitoring and Internal Compliance Audit

(a) The DU must create a compliance monitoring policy to ensure that all departments within the Private Hospital comply with the Principles of the PDPA and this Code.
(b) An internal compliance audit should be carried out by the DU at least once in Twelve (12) months to ensure that all policies and procedures relating to PD is adhered to the fullest by all personnel of the Private Hospital who handle and have access to PD in the Private Hospital.

8.3 Use of Medical Devices

(a) In a typical Private Hospital environment, numerous Medical Devices are used, such as X-ray Machines, CT Scanners, Ultrasound, MRIs and other similar devices, which record and store PD of the Patient. The Medical Devices generally retain a copy of the PD after transferring the PD to the Hospital Information Management System (HIMS).
(b) The DU should create policies relating to PD in these devices such that they are permanently deleted once the PD and images have been transferred to the HIMS.
(c) The DU should also ensure that the PD in these devices should be permanently deleted prior to decommissioning of the equipment or prior to sub-sale to a third party.

8.4 PDP Training

(a) The DU shall ensure that regular awareness training on the PDPA is carried out for all staff who have access to PD in the Private Hospital. This will include, doctors, nurses, consultants, administrative staff and all ancillary staff.
(b) For all new employees, PDPA awareness training should be included into the induction programmes when they first join the Private Hospital.
(c) For Private Hospitals that have a staff intranet system, regular tutorials on PDPA may be incorporated to bring awareness on a regular basis.

9. CODE REVIEW

(a) This Code may be reviewed every two (2) years or such other longer period as necessary as directed by the Personal Data Protection Commissioner.
(b) A review may be necessary to incorporate changes made to the PDPA, its Regulations or other legislation that has a direct impact on this Code.

10. CONCLUSION

(a) All DU must comply with this Code to the extent that it modifies or supplements that PDPA Principles.
(b) Where required, adequate internal policies must be developed to ensure that the PDPA and this Code is complied with fully.
(c) Existing policies should be reviewed to ensure compliance with this Code.

APPENDIX A
LIST OF PERMITTED DISCLOSURES

This list of permitted disclosures to 3rd Parties of the PD processed by a DU who is a Private Hospital.

This list is not exhaustive and may be added or amended to fulfil the "purpose" and for purposes directly related to the main purpose of providing .

No	Third Parties to whom disclosure is made by DU (Hospital)
1	Medical Specialists (as Data Processors) who run clinics and treat the DS in the Hospital
2	Insurance Companies that manage payment obligations of the DS
3	Managed Care Organisations that act as intermediary between employers and Insurance Companies in the payment process
4	Employers of the DS
5	Parents and Next of kin as permitted by the DS
6	Banks, Financial Institutions, Credit/Debit Card issuers for the processing of payments
7	Debt recovery agents to recover outstanding debt owed to the DU
8	Panel Lawyers who handle claims against the DU and provide advisory services to the DU
9	Private Laboratories s and diagnostic service providers who are outside the control of the Private Hospital environment
10	Data centres that host all Hospital Data for the DU
11	Agents, contractors and vendors who process data for the DU
12	External Auditors and Accountants
13	Approved bodies that collect employee benefits include: • Social Security Organisation (SOCSO) • Zakat • Employees Provident Fund • Lembaga Tabung Haji • Employees Insurance Scheme (EIS)
14	Federal Government and their Agencies and other related organisations • Ministry of Health • Ministry of Human Resources • Ministry of Home Affairs • Malaysian Anti-Corruption Commission • Inland Revenue Department • Malaysian Department of Insolvency • Royal Malaysian Police • Malaysian Medical Council (MMC) • Malaysian Dental Council (MDC) Malaysian Medical Association
15	Relevant Local Authorities

APPENDIX B

(NAME OF HOSPITAL)
PERSONAL DATA PROTECTION ACT 2010 DATA ACCESS REQUEST FORM

The following information is required to help us provide you a timely and accurate response to your Data Access Request pursuant to the PDPA 2010.

Full Name of Data Subject or Relevant Person	
Relevant Person's Relationship with the Data Subject	
Address	
Mobile Number	
E-mail address	

If you have been a Patient at the [Data User Hospital] please provide your Medical Record Number

If you are or have been employed at [Data User Hospital] please provide your Employment number and period of employment

Please provide details of the information you require from [Data User]:

Declaration: I am the Data Subject/Relevant Person named above and hereby request, under the provisions of Sections 12 and 30 of the Data Protection Act 2010, that [**Data User**] provide me with a copy of the personal data held about me as specified above. I understand that there may be a charge for this service and that [**Data User**] will contact me to request payment. I also note that the Hospital will respond within the time stipulated under the Act after receipt of payment from me and will notify me of a date and time to collect a copy of the documents personally.

Signed _____ Date _____