CLINICAL RESEARCH MALAYSIA (CRM) PERSONAL DATA PROTECTION GUIDELINES

1.INTRODUCTION

- The PDPA internal guidelines are created to ensure compliance with the Malaysian Personal Data Protection Act 2010 which came into effect on 15 November 2013.
- In this document certain legal terms are used and are defined below.
- The guidelines regulate the processing of personal data by Data Users/CRM and safeguards the rights of the Data Subjects and the Personal Data.
- Definition:

- Data Subject: Is the owner of the personal data processed;

- Data Users: Is a person who either alone or jointly or in common with other persons processes any personal data or has control over or authorises the processing of any personal data, but does not include a data processor;

- Data Processor: Any person other than the employee of the Data Users, who process the Personal Data solely on behalf of the Data Users and does not process personal data for his own purposes;

- Sensitive Personal Data: 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 similar nature, the commission or alleged commission by him of any offence or any other personal data as maybe determined by Minister of Communication and multimedia

2.NOTICE & CHOICE PRINCIPLE

- Data Users/CRM are required to make available written notice, also known as Privacy Notice, to Data Subjects prior to or as soon as possible after the collection of personal data. (The Privacy Notice is made available on CRM Official website).

- The Privacy Notice is a publicly available statement clearly expressing the privacy practices on how a Data User/CRM uses, manages, processes and discloses the personal data.

3.CONTENT OF THE PRIVACY NOTICE

- The Privacy Notice is to be communicated by the Data User to the Data Subject either when the first personal data being collected, when the Data User/CRM first requests the Data Subjects for the personal data or as soon as practicable thereafter.

***Situation/Example**: The provision/clause of an opportunity to view or read the applicable Privacy Notice via website address/link, prior to the submission of a web form containing personal data of the Data Subjects.*

4.MODES OF COMMUNICATING THE PRIVACY NOTICE

- Data User/CRM may communicate the Privacy Notice to the Data Subjects by one or more of the following methods:

1) By posting the Privacy Notice on CRM's website;

2) By issuing an e-mail to Data Subjects with a website address/link to the Data User/CRM(s)' Privacy Notice and /or telephone number to contact for further information;

3) By inserting a statement in application/registration forms (Business Development & Feasibility Form etc.) referencing the Privacy Notice, which may be accessed at a given website address/link, or by making a request to CRM's personnel/Data User;

4) By prominently displaying a summarized version of the Privacy Notice at CRM premises (e.g at the notice board, at the counter desk, at events or roadshows, or at a prominent location and making available the full Privacy Notice either upon a request being made at the counter or to CRM personnel;

- The Act requires Data User/CRM to maintain the evidence that the Privacy Notice was communicated to the Data Subject. Maintaining evidence on how the process of Privacy Notice is communicated to the Data User shall suffice.

Situation/Example 1: Where the Privacy Notice is communicated by email to Data Subjects, the production of relevant emails referencing the Privacy Notice, the Privacy Notice itself and the provision of the name of Data Subjects that the email was sent to, shall be sufficient to prove the Privacy Notice has been communicated.

Situation/Example 2: Where the Privacy Notice is communicated to Data Subjects by prominently displaying a summarized version of the Privacy Notice at the premises of the Data User's place of business and making available the full Privacy Notice at the counter, the production of the summarized Privacy Notice and the full Privacy Notice, shall be sufficient to prove that the Privacy Notice has been communicated to the Data Subjects.

5.WHEN CONSENT IS NOT REQUIRED

- **Consent is not required if the processing is:**

  - requested by the Data Subject with a view to enter into a Contract;
  - for performance of a Contract of which Data Subject is a Party;
  - to comply with any legal obligation to which the Data User is a Subject, other than the obligation imposed by a Contract;
  - to protect vital interest of the Data Subject;
  - for the administration of justice;
  - for the exercise of any functions conferred on any person by or under any law.

6.SECURITY

- Data User/CRM should take practical steps in order to safeguard the confidentiality, integrity and availability of Personal Data within the control of a Data User. The steps include implementing appropriate administrative, physical and technical measures to protect Personal Data from any loss, misuse, modification, unauthorized or accidental access, unauthorized disclosure, alteration or destruction.

- The practical steps are different from case to case, depending on the nature of Personal Data being processed by the Data User and the degree of sensitivity of the Personal Data or the harm that the Data Subject might suffer due to its loss, misuse, modification, unauthorized or accidental access, unauthorized disclosure, alteration or destruction.

- Data User should take reasonable and practical steps in implementing security measures to protect Personal Data within the control of a Data User, by taking into consideration of the following:

  (a) The nature of Personal Data and the harm that would result from such loss, misuse, modification, unauthorized or accidental access, unauthorised disclosure, alteration or destruction;
  (b) The place or location where Personal Data is stored shall not be exposed to physical and natural threats;
  (c) Any security measures incorporated into any equipment in which Personal Data is stored;
  (d) The measures taken for ensuring the reliability, integrity and competence of personnel having access to Personal Data; and
  (e) The measures taken for ensuring the secure transfer of Personal Data.

- CRM/Data User shall assess their existing policies and implement measures, including but not limited to the following:

(a) **Administrative**:-

(i) Confidentiality/Non-Disclosure Agreement;
(ii) Supervisory/monitoring personnel;
(iii) Training and education plan for personnel;

(b) **Physical**:-

(i) Door access system to control entry into and exit from premises where Personal Data is stored;
(ii) CCTV (if required);
(iii) 24 hours security surveillance (if required);
(iv) For Personal Data that is processed manually, the measures include:

-Filing of the Personal Data in an organized manner;

-Keeping files containing Personal Data in locked storage facilities and only one authorized person safekeep the keys;

-Keeping storage keys in a secured place/area; and

-Recording the movement of the storage keys.

(c) **Technical**:-

(i) Access authorization System;
(ii) Back Up/recovery System;
(iii) Anti-virus and anti-malware software; and
(iv) Encryption (if required).

- In addition, a Data User should consider implementing disaster recovery plans and business continuity plans to effectively secure Personal Data against any possible disaster and business interruption.

(d) Data Processing by Data Processor:-

-Data Processor is the engaged third party that processes personal data on behalf of CRM.

Example: Archiving Service Provider, IT System Service Provider, Accounting Service Provider, Postal Service Provider, Accomodation/Transportation Provider, Employees Medical Insurance Service Provider, Director's Insurance Service Provider etc.

-As part of security measures, CRM as the Data User shall provide Annual Questionnaire and Declaration by the Data Processor to the Data Processor on yearly basis.

7.RETENTION

- Personal Data processed for any Purpose shall not be kept longer than necessary for the fulfilment of the Purpose.
- It shall be the duty of CRM/Data User to take reasonable steps to ensure that all unused Personal Data is destroyed or permanently deleted if it is no longer required for the Purpose it was collected.

Example:

-Retention period for CV: 1 year

-Retention period for Payroll: 7 years

-Retention period of legal documents: 7 years

- Keep record of documents which have been destroyed:
  -description of documents;
  -disposal action taken;
  -who authorized the disposal;
  -who performed the disposal.

- If CRM were to outsource the disposal activity, must ensure that the destruction service is not limited to paper documents.

- All Personal Data in (electronic and non-electronic) must be disposed in a proper manner.

- Obtain certificate of destruction.

8.ACCESS

- A Data Subject shall be given their rights and access to:

-Their Personal Data; and

-The ability to correct the Personal Data if it is inaccurate, incomplete, misleading or not up to date

- CRM/Data User must comply with the data access request not later than 21 days.
- Any request in writing (i.e email/letter) is considered as valid request from the Data Subject, regardless of the format.

Schedule 1

To ensure compliance of PDPA, the following must be adhered to:

1. Determine if Consent is required before processing the Personal Data;
2. Obtain written consent before processing any Sensitive Personal Data;
3. Data User/CRM should inform the Data Subject on the PDPA Notice;
4. Ensure the Personal Data is used for its legitimate purpose only;
5. Keep all documents containing consents in a proper manner (i.e retrievable);
6. Keep paper files containing Personal Data locked in cabinets/storage;
7. Personal Data kept must be accurate, up-to-date and not misleading;
8. Avoid Personal Data tampering;
9. Ensure secured data transfer;
10. Avoid accidental disclosure;
11. Enter CDA/NDA prior to disclosing the Personal Data to authorized 3rd Party;
12. Delete permanently/destroy any unused CV.

Schedule 2

Things that **should not be done** as PDPA compliance:

1) CRM/Data User must not disclose any Personal Data through telephone calls, Internet, Instant Messaging, electronic communication, in writing or verbal unless consent is obtained from the Data Subject;

2) CRM/Data User must not leave unattended any hardcopy or soft copy of Personal Data;

3) CRM/Data User must not reveal password to unauthorized person;

4) Do not allow access of documents containing Personal Data unnecessarily to all personnel;

5) Do not view or discuss personal information in public;

6) Do not share log in credential with others;

7) Do not overshare on social media;

8) Do not collect personal data excessively. Enough if it is relevant with the nature of business;

9) Privacy notice placed at non-public area;

10) Improper storage of business contracts and financial documents.

Schedule 3

FAQ

Department	Issue
Clinical Operation	Study Coordinator: -The patients' information collected from hospitals' history database. i.e patients' age, disease etc. **[The PDPA did not apply as the database which the SC referred to was a general information and no person could be identified i.e statistic]** Clinical Operation Manager: -Should she delete all the resumes received from the applicants once the resumes have been forwarded to HR? **[Yes, proviso applies when she is involved in the selection process]** Recruitment Specialist: -Issue to state SC name and contact number in the protocol summary. Purpose: Referring patient from other institution. **[No issue if the SC is aware and involve in the Study]**
Feasibility	Feasibility Specialist: -Sharing of PI's email address to Sponsor/CRO? [**No issue it it is publicly available, if not then PI will have to be informed]**
Finance	Finance Executive: -Can CRM transfer the payment directly to the patient? [**Yes, as we are providing management of fund service]**