PUBLIC CONSULTATION FOR APPROACHES TO MANAGING PERSONAL DATA IN THE DIGITAL ECONOMY

Organisation:

Singapore Health Services

Contact Person:

Kwek Li Ling | Manager, GCOO's Office | Singapore Health Services

Address: 168 Jalan Bukit Merah, #16-01 Surbana One, Singapore 150168

DID: (65) 6377-7599

Email: kwek.li.ling@singhealth.com.sg

Question 1: Should the PDPA provide for Notification of Purpose as a basis for collecting, using and disclosing personal data without consent?

Feedback:

Yes. Presumably, the Notification of Purpose basis is in line with the notification clauses that MOH had formulated for use by PHIs in 2014, a copy of which is attached for the PDPC's reference in Annex A.

Question 2: Should the proposed Notification of Purpose approach be subject to conditions? If so, what are your views on the proposed conditions (i.e., impractical to obtain consent and not expected to have any adverse impact on the individual)?

Feedback:

Yes, the proposed Notification of Purpose approach should be subject to conditions.

From operational view, the conditions should be clear, easy to understand and implement. Ambiguity will result in multiple re-definitions and interpretations by organisations.

The conditions should be sector specific and dependent on legal or business purpose. For example, public healthcare institutions which are also Academic Medical Centre should be allowed to collect and use personal data where it is necessary to realise the legitimate interests of the organisation.

Will there will be a difference between "impracticability" for the research exemption and "impracticality" for the proposed Notification of Purpose approach and if so, how will the difference(s) be reconciled?

Will each sector be given the flexibility, and/or the relevant sector authorities (e.g. MOH for healthcare) roped in, to define "impracticality"?

Question 3: Should the PDPA provide for Legal or Business Purpose as a basis for collecting, using and disclosing personal data without consent and notification?

Feedback:

The "Legal or Business Purpose" basis kicks in when both consent and Notification of Purpose bases do not work.

Does PDPC intend to split this "Legal or Business Purpose" basis into two sub-limbs, and if so, whether the PDPC will stipulate an order of consideration i.e. organisations have to first consider the Legal Purpose and if that fails, then consider the Business Purpose?

Also, there's a need for clear guidelines on what conditions constitute to business purpose.

Question 4: Should the proposed Legal or Business Purpose approach be subject to conditions? If so, what are your views on the proposed conditions (i.e., not desirable or appropriate to obtain consent and benefits to the public clearly outweigh any adverse impact or risks to the individual)?

Feedback:

The 2 conditions proposed would need to be further clarified. What are the suggested guidelines on what is considered as 'not desirable', 'appropriate', 'benefits to public', 'adverse impact or risks to the individual'.

If a risk and impact assessment has to be done, at which level is this assessment done? At each individual level or according to a standard business process done at a high level? Could there be situations which may warrant repeated / periodic continuous assessment to be carried out?

Question 5: What are your views on the proposed criteria for data breach notification to affected individuals and to PDPC? Specifically, what are your views on the proposed number of affected individuals (i.e., 500 or more) for a data breach to be considered of a significant scale to be notified to PDPC?

Feedback:

How is the figure 500 derived? If a number has to be determined as a guide, should this number also vary according to sectors?

We are a PHI governed under MOH and they recently introduced a draft Data Incident Management Framework for Data Breach Incidents. MOH's Incident Management Framework appears to have a different definition on what is a significant scale of breach. Patient's health & financial information are given a higher severity compared to other personal identifiers such as NRIC, contact information, address, etc. How does PDPC plan to reconcile on the severity category? As different sector has its sectoral requirements, PDPC should harmonise these requirements.

Classification of Data Breach Incidents

Type of Personal Data Breached	Estimated No. of Affected Individuals	
	Less than 100	More than/ Equal to 100
Sensitive Personal Data Data breach could give rise to discrimination or any other negative impact against a person. E.g. A person's health information, financial information.	SEV 2	SEV 1
Other Personal Data Data breach is unlikely to give rise to discrimination or any other negative impact against a person. E.g. A person's contact information and personal data such as name, NRIC, contact number, email address.	SEV 3	SEV 2

Annex A

PERSONAL DATA PROTECTION ACT NOTIFICATION

We Respect and Keep Your Data Safe

The Personal Data Protection Act (PDPA) protects your personal data while enabling organisations to use your data reasonably to serve you. We, as a public healthcare institution, respect and keep your data safe by:

- limiting access to only doctors and healthcare personnel who are involved in your care, and the supporting internal processes,
- conducting regular checks to ensure only authorised persons have accessed your data, and
- removing details that identify you when using your data for internal purposes as far as possible.

Serving You as a Public Healthcare Institution

When you seek care at other healthcare providers, we will share relevant data with them through trusted information systems like the National Electronic Health Record (NEHR) system. We may use your personal data to invite you to participate in suitable care programmes, or shortlist you for participation in relevant research studies.

As a public healthcare institution, we share relevant data and participate in national and multi-agency efforts to:

- review healthcare policies and requirements,
- review programmes that ensure patient safety and improve the quality of healthcare services,
- conduct disease surveillance to address public health concerns, and
- train future generations of healthcare professionals.

Please be assured that if your personal data is collected, used or disclosed for these purposes, we will protect it as required under the PDPA and other relevant legislation such as the Private Hospitals and Medical Clinics Act.