PDPC's Public Consultation on Personal Data Protection (Amendment) Bill 2020

Feedback provided by National University Health System

28 May 2020

Contact:

NUHS Data Governance & Protection Office

(1) Chris Ng
Group Chief Data Governance and Protection Officer
Email: Chris_HB_NG@nuhs.edu.sg

(2) Aidah Jahari
Manager
Email: Aidah_jahari@nuhs.edu.sg

28 May 2020

To: The Personal Data Protection Commission

Re: Public Consultation on PDP (Amendment) Bill 2020

PART II: STRENGHTHENING ACCOUNTABILITY

1. **New Part VIA**

Clause 12 of the draft Bill: Notification of Data Breaches (Section 26A- 26D of the New Part VIA)

Public Healthcare Institutions ("**PHIs**") have adopted the Ministry of Health' ("**MOH**") personal data breach incident management and reporting framework (**MOH Circular No. 18/2018**). This framework covers all entities that are under MOH's supervision.

PHIs have set up specific processes for reporting and managing personal data breach incidents, which includes determination of the personal data breach incidents' severity category, reporting/ escalation process, internally and to MOH. MOH will assess the breach and advise the PHI whether or not to notify PDPC and the affected individuals of the data breach. Criteria for notification is based on whether the breach results in significant harm to the individuals or to the organisation or is of significant scale (equal to or more than 100 individuals' data). It is noted that the numerical threshold on what constitutes "a significant scale" that PDPC intends to prescribe in its regulations based on its past enforcement cases is 500 or more. The MOH framework also establishes timelines for investigation, reporting, escalation and notification of a data breach, and provides categories of non-reportable incidents.

For PDPC's consideration:

(a) To avoid significant changes and disruptions to PHIs exiting data breach management and escalation processes, we recommend PDPC and MOH to align the new proposals relating to breach notification criteria, data breach assessment, notification timeframes, and notification exceptions with existing MOH's data breach incident management and reporting framework. PDPC to clarify whether the MOH Circular will be applicable after the new proposals are implemented.

(b) PDPC to prescribe healthcare specific regulations for categories of personal data that require notification to affected individuals, which if compromised could result in significant harm to individuals.

(c) PDPC to include non-reportable incidents stated in MOH's Circular No. 18/2018 as exceptions to the requirement to notify affected individuals.

(d) Section 26C (3) of the New Part VI A of the draft Bill provides that organisations must carry out data breach assessments in accordance with any prescribed requirements. The Guidelines to Managing Data Breaches 2.0 issued by the PDPC provide that organisations are to carry out their assessment of data breaches expeditiously within 30 days from when they first became aware of a potential data breach. PDPC to clarify whether the Guidelines to Managing Data Breaches 2.0 constitute "prescribed requirements" for the purposes of Section 26C (3).

(e) To define what unauthorised disposal of personal data means. Is the incorrect administrative disposal of personal data (e.g. disposing in general waste instead of shredding) considered a data breach?

(f) Need guidance on what constitutes a reasonable belief that a data breach has occurred. For example, a staff member cannot remember where a secured laptop with personal data was last seen. What is a reasonable time period of discovery before we conclude that a data breach has occurred?

(g) What information should the notification(s) to PDPC and affected individuals contain? A reporting template would be useful to ensure consistency.

(h) Is the day the incident was reported considered as Day 0?

(i) How does subsection (6) of Section (26D) apply if the breach meets the criteria for subsection (4) and/or (5)? Are organisations required to wait for further instructions from the prescribed law enforcement agency or Commission before they notify the affected individuals? If so, it might lengthen the time from the day of reporting.

Attachments for PDPC's review.
Annex 1 – MOH Circular No. 18/2018 (Personal Data Breach Incident Management and Reporting Framework)

2. **Amendment of section 4 (Principal Act)**

Clause 3 of the draft Bill: Removal of exclusion for organisations acting on behalf of public agencies (Section 4 (a)).

Currently, an organisation in the course of acting on behalf of a public agency in relation to the collection, use or disclosure of personal data is excluded from the application of the PDPA provisions. The PDPA will be amended to remove the exclusion for organisations that act on behalf of a public agency.

For PDPC's consideration:

(a) PDPC to exclude PHIs or any other data intermediary (e.g. IHiS) from the application of PDPA when they are mandated to assist in the extraction of medical data of patients under specific legislation such as the National Registry's Act.

3. **New Part VIIIA**
Clause 20 of the draft Bill: Offences related to:
(a) **Unauthorised disclosure of personal data** (Section 35 B(1)(c) of the New Part VIIIA)
(b) **Improper use of personal** (Section 35 C(1)(c) of the New Part VIIIA)
(c) **Unathorised re-identification of anonymised information** (Section 35 D(1)(c) of the New Part VIIIA)

PDPC proposes to introduce criminal sanctions on individuals who mishandle personal data in the possession of or under the control of an organisation or a public agency, and will hold an individual accountable for:

- knowing or is reckless that the disclosure of the personal data is unauthorised.
- knowing or is reckless that the use of the personal data is unauthorised.
- knowing or is reckless that the re-identification of the personal data is unauthorised

For PDPC's consideration:

(a) PDPC to clarify when an individual is deemed to be reckless and liable in the healthcare context and in light of the PDPC's SingHealth decision.

(b) The word "reckless" should be defined.

(c) As organisations will primarily be held accountable for data protection, PDPC to clarify the circumstances when an organisation shall remain liable for the actions of their employees.

(d) Does this supercede the Official Secrets Act with respect to PHI employees?

(e) Is the burden of proof on the organisation or on the individual to prove that the action was unauthorised?

(f) Does the "gain" in section (35C) need to have a monetary or implied monetary value? Will the unauthorised use of data for personal research, or to meet the requirements of academic research, constitute a gain to himself or another person?

(g) To confirm that section (35D) does not criminalise spontaneous recognition of anonymised data subjects, or poor anonymisation practices such that the recipient of the data would easily be able to re-identify the data subjects because of their specialist knowledge. (e.g. an anonymised list of rare disease sufferers, where the relevant medical expert is familiar with all of the cases)

(h) To confirm that section (35B (3)) is also applicable to those who are required to disclose the data due to legal/court proceedings, even if it is a civil suit?

PART III: ENABLING MEANINGFUL CONSENT

1. **Amendments of Section 15 (Principal Act)**

Clause 6 of the draft Bill: **Deemed Consent by Contractual Necessity** (Section 15 (3) & (4))

The proposed amendments provide that consent may be deemed to have been given by an individual when his/her personal data is disclosed to or used by a third- party organisation to conclude or perform a contract or transaction.

For PDPC's consideration:

(a) PDPC to clarify who are the "third-party organisations" contemplated in the context of healthcare sector, and provide examples on the application of the new provisions.

(b) Healthcare specific sectorial guidelines is recommended to better understand the application of the new provisions. PDPC to work with healthcare industry and MOH to develop the sectorial guidelines.

2. **New Section 15A**

Clause 7 of the draft Bill: Deemed Consent by Notification (Section 15A 1-4).

Public Healthcare Institutions (PHIs) currently rely on MOH's Notification for deemed consent for the collection use and disclosure of patient data. The Notification is displayed in patient facing areas (e.g., ED, Wards, SOC clinics), and supports the current provisions on deemed consent, where the patient is deemed to have consented to the collection, use and disclosure of his personal data when he voluntarily provides the data for the purpose of treatment and care.

The Notification informs the patients on the possible uses of their data but does not give the individual an opportunity to "opt-out" from the collection use or disclosure of their personal data. If the patients are given the opportunity to "opt-out", then hospitals will not be able to treat patients who exercise this option. PDPC is proposing to introduce deemed consent by notification to include an opt-out option for individuals who do not wish their data being collected under the notification.

Also, currently PHI's follow MOH's guidelines on withdrawal of consent ("**Consent Withdrawal Communications" (for PHIs)**). MOH's guidelines provide that patients are only permitted to withdraw their consent from data being accessed from MOH's National Electronic Health Record system ("**NEHR**"). They cannot withdraw consent at hospital level where they are being treated, as withdrawal of consent for the collection use and disclosure of data would mean that the hospital would not be able to treat them.

For PDPC's consideration:

(a) The new section 15A 3(iii) (opt-out option) should not apply to healthcare institutions for the reasons stated above. The PHIs have processes in place to handle "withdrawal consent", and these should remain status quo.

(b) The current MOH Notification for deemed consent should be amended and aligned to include the proposals for the expanded deemed consent, i.e. deemed consent by contractual necessity and notification as well as PHIs to be able to use personal data collected for quality assurance, service improvements and for programmes that ensure patient safety and improves the health of the population.

Attachments for PDPC's review.
(a) Annex 2 – MOH Notification
(b) Annex 3 - Consent Withdrawal Communications (for PHIs)

3. New First Schedule

i. Clause 31 of the draft Bill – Matters affecting the public (Part 2)

The amendments will streamline and consolidate the exceptions to consent, to simplify how organisations may collect, use and disclose personal data without consent.

For PDPC's consideration:

a) This section seems to suggest that the disclosure of personal information for the purposes of news is an exception to consent. In the medical domain, patients and their conditions should be treated with extra care and personal medical data in this case should not be exempted from consent if the purpose is for news.

b) What if the publicly available personal data is due to doxxing?

ii. Clause 31 of the draft Bill – Legitimate interests' exception (Part 3, 1(1) - (5))

This new exception is intended to enable organisations to collect, use or disclose an individual's personal data without consent in circumstances where it is in the legitimate interests of the organisation and the benefit to the public is greater than any adverse effect on the individual.

For PDPC's consideration:

(a) PDPC to clarify whether this exception can apply to the collection use and disclosure of an individual's personal data for programmes relating to the improvement of population health and other regional health system programmes which are clearly run to benefit the public.

(b) PDPC to issue a healthcare specific sectorial advisory guidelines to better understand the application of this exception in the healthcare context with relevant examples.

4. **New Second Schedule**

Clause 32 of the draft Bill – Business improvement exception (Part 2, 2(1) -(2))

This new exception is intended to enable organisations to use personal data collected without consent for business improvement purposes.

For PDPC's consideration:

(a) PDPC to clarify whether data can be shared by organisations with third parties under this exception for the purpose of developing and improving their business processes.

(b) PDPC to issue a healthcare specific sectorial advisory guidelines to better understand the application of this exception in the healthcare context with relevant examples.

PART IV: INCREASING CONSUMER AUTONOMY

1. New Part VIB

Clause 13 of the draft Bill: **Data Portability Obligation** (Section 26E-26H of the New Part VIB)

Under this obligation, an organisation must at the request of an individual, transmit his/her personal data that is in the organisation's possession or under its control, to another organisation in a commonly used machine – readable format.

For PDPC's consideration:

(a) PDPC to clarify how does a request for data portability be managed by an institution when the data system is shared by more than one institution and the individual may be a patient in different institutions that share the data system. For e.g., the NGEMR will be shared by institutions of two clusters, NHG and NUHS. The individual may be a patient of both clusters, but the patient has one record in the system. Does the patient need to make a data porting request to both clusters? As the patient has one record in the shared system, then which cluster will be responsible for executing the patient's request or be accountable to the patient?

(b) Currently, PHIs transmit patient data to the National Health Electronic Record System (NEHR), which is owned by MOH Holdings (MOHH). PDPC to clarify whether patients can request their data to be ported from NEHR? If yes, then the request should be made directly to MOHH and not to a healthcare institution.

(c) PDPC to clarify and ensure the burden to comply with this obligation is reasonable for PHIs. The issuance of regulations on data portability should be healthcare specific.

(d) Subsection (26G (5)), PDPC to clarify what is defined as excluded class of applicable data?

(e) Subsection (26G (6)), how about data that may potentially be needed for legal/court proceedings?

(f) Subsection (26G (6c)), are organisations required to seek further instructions from the Commission before we transmit any data? If so, it might be a lengthened time from the day of request received.

PART V: STRENGTHENING EFFECTIVENESS OF ENFORCEMENT

1. Amendment of section 29 (Principal Act)

Clause 17 of the draft Bill: **Increased financial penalty cap** (Section 29 (2)(d))

PDPC has proposed to increase the financial penalty for data breaches; (i) up to 10% of an organisation's annual gross turnover exceeding $10 million; or (ii) in any other case - $ 1 million.

For PDPC's consideration:

(a) PDPC to clarify whether the cap of $1 million financial penalty is applicable to healthcare institutions or whether healthcare institutions could be liable to a maximum financial penalty of 10%.

PART VI: OTHERS

1. Amendment of section 21 (Principal Act)

Clause 10 of the draft Bill: **Prohibitions to providing access** (Section 21 (3A))

The proposed amendment will allow organisations to provide access to data that could (i) reveal personal data about another individual, or (ii) reveal the identity of an individual who has provided the personal data about another individual and that individual does not consent to the disclosure of his/ her identity.

For PDPC's consideration:

(a) Organisations may be subject to receiving complaints if personal data of third party individuals is revealed without their consent to the person who makes an access request to the organisation. PDPC to clarify how organisations may deal with such complaints.

(b) PDPC to clarify whether it will be necessary to remove or mask images of third party individuals captured in CCTV footage when a person requests to access his CCTV footage.

(c) Reference to point (3A), if the disclosure of data might cause harm or embarrassment to a third party individual, are organisations still required to provide such access?

(d) PDPC to provide more clarity on the prescribed time and requirements to notify the requestor.

The following annexes are attached in the email:

i. **ANNEX 1**
MOH Circular No. 18/2018 (Personal Data Breach Incident Management and Reporting Framework)

ii. **ANNEX 2**
MOH Notification

iii. **ANNEX 3**
Consent Withdrawal Communications (for PHIs)

MINISTRY OF HEALTH (MOH) NOTIFICATION

(TO SUPORT THE COLLECTION, USE DISCLOSURE OF PATIENT DATA BASED ON DEEMED CONSENT)

NOTIFICATION CLAUSES FOR PUBLIC HEALTHCARE INSTITUTIONS

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.

CONSENT WITHDRAWAL COMMUNICATIONS

(for Public Healthcare Institutions)

What if a patient wants to withdraw consent?

Under the PDPA, patients may, by giving reasonable notice, indicate that they wish to withdraw consent for the PHI to collect, use and disclose their personal data. PHIs are obliged to evaluate the request, and inform the patient about how the withdrawal of consent may affect the care and services they receive from the PHI, as well as whether and how PHIs may accede to the withdrawal request.

However, PHIs should also bear in mind that under the PHMC Act and the regulations made thereunder, healthcare institutions are obliged to maintain medical records of patients that are complete, accurate and up-to-date. In addition, under the SMC Ethical Code and Ethical Guidelines ("ECEG"), doctors are obliged to maintain their medical records and ensuring that these are in good order in the event that the patient is transferred/referred subsequently to another doctor or institution.

Hence, it is not possible for patients to request that institutions delete their personal information as it is not permitted under the PHMCA and there is no legal obligation to do so under the PDPA. Patients may however request that their records are not made accessible via the NEHR, or are not shared further with other institutions or for other purposes not directly relating to their treatment and care.

Four possible scenarios in which patients may refuse consent are given below, together with the proposed patient communications position for each.

Proposed Patient Communications Position

1. To a general request to withdraw consent for collection and use of personal data

Under the PHMC Act, institutions have to maintain complete and accurate medical records. Likewise, doctors are required as a matter of professional conduct to maintain complete and accurate medical records. Proposed line of response as follows:

"We take patient confidentiality very seriously. We collect, use and disclose your personal data only where necessary and appropriate for the purposes of your care (including for referrals to other healthcare professionals and institutions) and other associated purposes (e.g. billing and internal administration), and allow access only by persons involved in your care for these purposes.

Your medical records are maintained primarily to ensure that we can provide safe and appropriate care to you and also to ensure the completeness and accuracy of the medical records we hold. This is also required in order for us to meet our business and legal requirements, and is permissible under the PDPA. As such, it will not be possible for you to withdraw consent for us to collect or use your

data so long as you are or have been a patient with our institution. For the same reasons, it will not be possible for us to delete or destroy your medical records with us."

2 If patient wants to withdraw consent to the institution sharing data via NEHR or directly with other providers/institutions

Proposed line of response as follows:

"We only make your data available to other healthcare professionals and institutions in support of your care. This has many benefits, as it allows other doctors you consult to better assess how to treat you by knowing your past conditions, including ensuring that the medication you receive is suitable for you and that you are not required to undergo unnecessary repeat tests. This enhances the care you receive and reduces the costs and inconvenience to you. Doctors are also professionally obliged to share such information with their colleagues to ensure a smooth transfer when they refer patients to one another. Therefore, it is in your interests to facilitate the sharing of such information, including keeping your information on our health IT system, including the NEHR."

(If the patient persists in the request to withdraw consent for sharing of data)

Patients are currently allowed to opt out of the NEHR, but this may be rather unnecessary and extreme to equate with withdrawal of consent.

The NEHR is basically a data repository offering access on the basis of "implied consent" to facilitate a patient's consultation with the doctor for care and treatment. The doctor is expected to check with the patient before accessing the patient's records, and the patient would have some level of control over the doctor's access to his NEHR records. The same access protocols also apply to EMRX and similar data sharing systems.

"If you withdraw your consent, we will no longer allow your personal data to be disclosed to other healthcare organisations, including your future healthcare providers, unless we are allowed or required to do so under applicable laws or government requirements. We would encourage you to not block such access in your own interests. In future, if you would like your future providers to make use of this data, you would have to write back to us to inform us that you agree to allow your personal data to be disclosed."

[Institution should include some pointers here on their own process for individuals who withdraw consent for sharing data on NEHR. As sharing of information also takes place on EMRX, institutions are reminded to check with patients during their visits that they are agreeable to their records being accessed via EMRX.]

3. If the patient does not want students/trainees (e.g. medical students) to treat/see them

Institutions should manage the patient as is currently per current practice, to advise them that as a public healthcare institution, training is part and parcel of their business and that students and trainees are required to maintain patient confidentiality just like their full-fledged counterparts. They are also not allowed to keep identifiable notes of patients they see.

4. If patients do not want their data included for PHI's research purposes.

As this is a legitimate request, PHIs would need to respect the patient's wishes.

Extracts of "Personal Data Protection Act 2012" on Withdrawal of Consent

Withdrawal of consent

16.—(1) On giving reasonable notice to the organisation, an individual may at any time withdraw any consent given, or deemed to have been given under this Act, in respect of the collection, use or disclosure by that organisation of personal data about the individual for any purpose.

(2) On receipt of the notice referred to in subsection (1), the organisation concerned shall inform the individual of the likely consequences of withdrawing his consent.

(3) An organisation shall not prohibit an individual from withdrawing his consent to the collection, use or disclosure of personal data about the individual, but this section shall not affect any legal consequences arising from such withdrawal.

(4) Subject to section 25, if an individual withdraws consent to the collection, use or disclosure of personal data about the individual by an organisation for any purpose, the organisation shall cease (and cause its data intermediaries and agents to cease) collecting, using or disclosing the personal data, as the case may be, unless such collection, use or disclosure, as the case may be, without the consent of the individual is required or authorised under this Act or other written law.

Retention of personal data

25. An organisation shall cease to retain its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that —

(a) the purpose for which that personal data was collected is no longer being served by retention of the personal data; and

(b) retention is no longer necessary for legal or business purposes.

Extracts of PDPC Advisory Guidelines on Key Concepts in the Personal Data Protection Act

Withdrawal of consent

12.39 Section 16 of the PDPA provides that individuals may at any time withdraw any consent given or deemed to have been given under the PDPA in respect of the collection, use or disclosure of their personal data for any purpose by an organisation.

12.40 Section 16 sets out a number of requirements that must be complied with by either the individual or the organisation in relation to a withdrawal of consent. In brief, they are:

a) the individual must give reasonable notice of the withdrawal to the organisation (section 16(1));

b) on receipt of the notice, the organisation must inform the individual of the consequences of withdrawing consent (section 16(2));

c) an organisation must not prohibit an individual from withdrawing consent, although this does not affect any legal consequences arising from such withdrawal (section 16(3)); and

d) Upon withdrawal of consent, the organisation must cease (and cause its data intermediaries and agents to cease) collecting, using or disclosing the personal data, as the case may be, unless the collection, use or disclosure of the personal data without consent is required or authorised under the PDPA or any other written law (section 16(4)).

Organisations must allow and facilitate the withdrawal of consent

12.41 In general, organisations must allow an individual who has previously given (or is deemed to have given) his consent to the organisation for collection, use or disclosure of his personal data for a purpose to withdraw such consent by giving reasonable notice. In this regard, considerations for whether reasonable notice has been given would include the amount of time needed to give effect to the withdrawal of consent and the manner in which notice was given.

12.42 In order to enable and facilitate withdrawal, organisations are advised to make an appropriate consent withdrawal policy easily accessible to the individuals concerned. This withdrawal policy should, for example:

a) advise the individuals on the form and manner to submit a notice to withdraw their consent for specific purposes;

b) indicate the person to whom, or the means by which, the notice to withdraw consent should be submitted; and

c) distinguish between purposes necessary and optional to the supply of the good/services or the service of the existing business relationship. (Individuals must be allowed to withdraw consent for optional purposes without concurrently withdrawing consent for the necessary purposes).

12.43 Organisations should not have inflexible consent withdrawal policies that seek to restrict or prevent individuals from withdrawing consent in accordance with the PDPA.

12.44 An organisation must not prohibit an individual from withdrawing his consent to the collection, use or disclosure of personal data about the individual himself. For example, if an organisation requires certain personal data from an individual in order to fulfil a contract with the individual to supply products or services, it may not stipulate as a term of the contract that the individual cannot withdraw consent to the collection, use or disclosure of the individual's personal data for the purposes of the contract. If the individual subsequently withdraws consent to his personal data in a manner which makes it impossible for the contract to be fulfilled, any legal consequences arising out such withdrawal would not be affected.

Actions organisations must take upon receiving a notice of withdrawal

12.45 Once an organisation has received a notice to withdraw consent, the organisation should inform the individual concerned of the likely consequences of withdrawing his consent. Consequences for withdrawal of consent could simply be that the organisation would cease to collect, use or disclose the individual's personal data for the purpose specified by the individuals, or that the organisation would be unable to continue providing services to the individual.

12.46 Organisations should note that they must highlight the consequences of withdrawal to individuals upon receipt of their notice to withdraw consent even if those consequences are set out somewhere else – e.g. in the service contract between the organisation and the individual.

12.47 With regard to personal data that is already in an organisation's possession, withdrawal of consent would only apply to an organisation's continued use or future disclosure of the personal data concerned. Upon receipt of a notice of withdrawal of consent, the organisation must inform its data intermediaries and agents about the withdrawal and ensure that they cease collecting, using or disclosing the personal data for the organisation's purposes.

12.48 Apart from its data intermediaries and agents, an organisation is not required to inform other organisations to which it has disclosed an individual's personal data of the individual's withdrawal of consent. This does not affect the organisation's obligation to provide, upon request, access to the individual's personal data in its possession or control and information to the individual about the ways in which his personal data may have been disclosed. Hence the individual may find out which other organisations his personal data may have been disclosed to and withdraw consent to them directly.

12.49 Although an individual may withdraw consent for the collection use, or disclosure of his personal data, section 16 does not require an organisation to delete or destroy the individual's personal data upon request. Organisations may retain personal data in its documents and records in accordance with the Data Protection Provisions. For more information on this, please refer to the section on the "Retention Limitation Obligation".