PDPC's Public Consultation on Proposed Data Portability and Data Innovation Provisions

Submission by Singapore Health Services Pte Ltd (SingHealth)

Contact SingHealth Data Protection Office: pdpa@singhealth.com.sg

Comments on Proposed Data Portability Obligation

Q1. What are your views on the impact of data portability, specifically on consumers, market and economy?

As public healthcare providers, much of our patients' health records are already shared with other healthcare providers via the National Electronic Health Records (NEHR) system to enable authorised healthcare professionals to have a holistic view of a patient's healthcare history.

If the proposed Data Portability Obligation is to be also applied to the healthcare sector in Singapore, possibly the general impact would be as follows:

Consumers

- In greater position to make unilateral decision about the medical services they require
- Encourage patients to switch from one healthcare provider to another i.e. the practice of 'doctor hopping' based on benefits like shorter waiting time or just to try out
- Disruption of care
- Overconsumption of healthcare services
- Greater financial burden

Market and Economy

- Encourage resources to be channeled into data migration or extraction
- Unless appropriately referred by medical professionals, overconsumption of healthcare services can happen if patients' medical conditions do not warrant a referral
- Skewed results due to erroneous interpretation or analysis of medical diagnostic data by inexperienced sources e.g. third party wellness company would result in no benefit to greater population health

Clarifications required:

i. *Does this porting provide the individual (eg low income earners) to potentially sell his own data when incentivized through vouchers, free medical check up, money.*

Q2. What are your views on the proposed Data Portability Obligation, specifically –

a) scope of organisations covered;

Clarifications required:

i. *Would SingHealth institutions be considered as "Any organisation in the course of acting on behalf of a public agency in relation to collection, use or disclosure of personal data" under section 2.16 (d) of the "Covered organisation"?*

ii. *Are we obligated to share our data to non-healthcare organisations if patient wants us to?*

b) Scope of data covered?

- Processes within healthcare largely require human interactions and the sensitive and complex data generated tend to be difficult to standardise.

- Data come from many different data sources (OAS, SAP, SCM, etc.) and extensive manpower is required to extract, and check and ensure that the data is complete and accurate before transferring to another organisation.

- Compliance cost will increase greatly.
  - E.g. Some service providers use imaging system extensively like Ophthalmology
    - Image acquisition system software is not a common software like Word, PDF, Excel or common machine readable format for example, CT, and X ray.
    - Eye image file sizes (e.g. scan of retina nerve fibre layer) are too huge (10MB) and cannot be easily transmitted via email.

- In terms of patient medical records and data, differentiating between electronic and non-electronic for data portability obligation may lead to incomplete medical information being transferred which could entail risks and safety concerns.

- Patients and public may therefore demand all data (electronic or non-electronic) to be made portable which would require immense resources to fulfill (increasing compliance cost) or if unfulfilled, lead to complaints and PR issues.

- Besides medical information, communications with patients over email and social media are also included and this would be laborious to retrieve.

- Patients' activity directly and indirectly contributes to derived data for Quality Improvement and Service Quality. It would not be easy to differentiate between user activity data and derived data.

- Scope of data covered proposed may be insufficient when applied to healthcare and healthcare related data. The definitions provided (User Provided Data, User Activity Data, and Derived Data) only generally frame the kind of data healthcare institutions have collected/retained/used.

- Based on the examples given for user provided, user activity and derived data, data included in scope could potentially be classified as follows:

Type of Information	Data Subject to Data Portability Obligation		Data not subject to Data Portability Obligation
	User Provided Data	User Activity Data	Derived Data
Patient	Patient Registration Information (Name, contact details, NRIC number, Credit Card information, profile information)	• Date, timings and transactions made during a patient visit • Medical information including drugs/treatments prescribed • Tests ordered • Locations of appointments • Raw results of a patient's diagnostic testing • Patient feedback scores	• Medical Report • Diagnosis of patient's condition • Results/findings yielded from Clinical investigations/ Research • Trends from analysed patient feedback scores • Trends predicted/ reported from drug usage/ prescription • Information/ data related to Morbidity and Mortality • Workload/ utilisation trends analysed from patient activity • Information relating to success of treatments/ medical devices
Staff	Employee information (Name, address, professional qualifications, vaccination details)	• Professional achievements • Information related to job specific qualifications • Vaccination details • Job scope/ responsibilities	• Performance appraisal information
External Parties (Vendor/Visitor Information Including: Clinical observers, attachments, medical/nursing students, Conference delegates, event vendors/visitors, research sponsors, external auditors /agencies etc.)	Visitor/vendor information • For purposes of exchange of security passes • Information collected in the process of ongoing tender, or for services rendered • Contact information • Professional qualifications • Vaccination details	• Date, timings and frequency of visits • Information related to job-specific qualifications • Vaccination details • Education information • Vaccination details • Professional achievements	• Medical student intake trend • Performance appraisal information • Trends analysed from information relating to overseas engagements

- Patients' Next-of-kin or caregiver information could be sensitive and would require consent to be shared under Data Portability Obligation.

Clarifications required:

i. *What is the standard in healthcare for machine readable format to ensure compatibility when sending and receiving information?*

ii. *With no predefined standard, as a receiving organisation, do we have to cater to all available formats, e.g. if a patient requests to port his medical records from one PHI to another (when he/she decides to change his doctor). How does a NHG institution port a patient's medical records over to a SHS institution or vice versa, when they are not interfaced?*

iii. *How will user activity be defined for healthcare?*
   - *Will medical notes, clinical data, records, diagnosis, images, X-rays be considered to be generated by the hospital and not as direct user activities?*
   - *Should user activity data in healthcare setting include information such as 'date and time and location' of patients at specific clinics, tests/ investigations rooms, operating rooms etc, and such information on type of tests, procedures/surgery done? (This could contain highly sensitive and confidential information e.g. HIV, abortions, etc.)*

iv. *How will the portability request apply to medical information and NEHR? E.g. if the information is on NEHR, will there be a special exclusion?*

v. *Does electronic data refer to information that is captured in discrete machine readable data as opposed to digitised/scanned documents from originally physical documents? (It would be impractical to provide digitised images in any meaningful way to a third party.)*

vi. *How granular should the data be to ensure patient safety?*
   - *Should we provide casemix level information?*

vii. *Patients seem to be allowed to pick and choose what is to be shared, para 2.37 (c). Isn't this a disservice to patients?*

viii. *Receiving party can choose to reject full or partial data received. This suggests that effort must be made to screen through the data to decide what to retain or reject. Do we allow incoming data to overwrite what we have on record? Who decides whose data is cleaner or dirtier?*
   - *Potential for dirty data to overwrite clean ones.*

- *Issue of patient safety surfaces as our clinicians may prescribe healthcare based on data received yet there is no source of truth verification done.*

ix. *Does it mean that all data collected by Public Healthcare Institutions (PHIs) under Private Hospitals and Medical Clinics (PHMC) Act are not subjected to the Data Portability Obligation since Annex A states that the proposed data portability obligation does not apply to data collected without consent or where required or authorised under the PDPA or other written law?*

x. *Would there be exclusions to disclosure for high stake conditions and results from any genetic/genomics testing and ensuing diagnosis?*

xi. *Would certain special individuals or groups be excluded from this obligation?*

xii. *For contractual agreements that indicate no data sharing outside of the contract, would these be excluded from this obligation?*

xiii. *What will be the implication of this data portability obligation in Legal terms, especially if the originating Institution gave wrong/ insufficient assessment? Will these information be ported over as well? The means to port the data over will depend on how the hospital systems are configured. Do we have enough resources to ensure that the data ported over is "clean"? Are we then opening ourselves to being sued by the individuals if data ported over contain more information that should not be ported?*

xiv. *Does Data Portability Obligation include Patient Data stored in SingHealth systems, eg, if patient wants his health data for admission to private/overseas hospital? If yes, which type of data requests that hospitals need to handle?*

Q3. What are your views on the proposed exceptions to the Data Portability Obligation, specifically –

a) the proposed exception relating to commercial confidential information that could harm the competitive position of the organisation, to strike a balance between consumer interests and preserving the incentive for first movers' business innovation;

- Necessary to safeguard novel findings from clinical investigations and research or other commercial information.

Clarifications required:

i. What are the parameters/guidelines to decide what is considered competitive position?

b) and the proposed exception for "derived data"?

- According to the definition, most medical information aside from patient history and raw test results would be considered derived data.

- The definition of medical information as derived data must be agreed by the cluster.

Clarifications required:

i. *Are opinions and recommendations of clinicians considered 'derived data'? For example, if the record shows that the patient has a diagnosis of "personality disorder" is this patient provided data, an observation or is this the opinion of the doctor derived from his observations of the patient?*

Q4. What are your views on the proposed requirements for handling data portability requests?

- It depends on the type and nature of the data request to be ported.

- Onerous burden on the organisation.
  - Additional resources and costs to handle the request, process and transfer with the patient and receiving organisation as there is a requirement for requesting individual to verify the data before transmission
  - Introduction of a number of business processes and maybe new IT system/process to manage the requests as it only applies to electronic data.
  - Requesting individuals should be charged with the responsibility to clearly specify which data to be ported and which not to be ported or removed to enable the organisation to execute the request.
- There should also be more flexibility for fees chargeable and timeline for completion depending on the nature of the data to be ported as some may be complex and will require much greater time and effort.

- For medical reports, processes in place for verification of requests which require the patients/collector's ID to be sighted before the release of medical reports.
  - According to SingHealth regulations, we are obligated to send/release information to the within 30-days.
  - Hence, the limitation of a 7-day transfer period is unrealistic as we would need to ascertain the means by which data could be securely transferred, and that the medium of data is acceptable to the receiving organisation.

- Much of patient provided information/directly observed data is mixed with clinical opinions of the clinician generating the document.
  - It is difficult to provide all the information in an electronic machine readable format.
  - Also, the information is subject to interpretation based on the context of the individual patient.
  - Need guidance from sector regulators to have a standardised format (e.g. results and medical information) to be provided in machine readable formats and details of clinical consultations/interactions to be provided in the form of a medical report for consumer related purposes (as opposed to medicolegal proceedings).

Clarifications required:

i. *Para 2.37 point c 'Verifying the data to be ported': If the data to be ported concerning assessment and the requesting individual wishes for assessments and negative feedbacks that may affect the overall performance to be removed, are they able to do so? Will the organisation be able to reject the request due to data integrity issue?*

ii. *On data security: How can the data be verified and transmitted seamlessly without compromising quality of the data and potential threats?*

iii. *Will there be an aligned request and transfer process/mechanism for Singhealth, for healthcare-to-healthcare (public and private) and healthcare-to-extended partners / private organisations? E.g. request process and cost, transfer medium, requester identity verification, etc.*

Q5. What are your views on the proposed powers for PDPC to review an organisation's refusal to port data, failure to port data within a reasonable time, and fees for porting data?

- PDPC has the rights to conduct such reviews and/or necessary audits.
- Helpful to have guidelines for reference specific to industry or sector.
- The healthcare industry is already routinely providing patients copies of their medical information and medical reports when requested. As long as the timelines are reasonable taking into account the resources allocated this should be achievable.

- The pricing cost may not be so straight forward for healthcare data that may not be kept in 1 system or will take much effort to extract. Logistical challenges in extracting data may impact ability to port data in the requested 7 calendar days.

- Fees should be capped to prevent organisations from charging a cost that is not economically feasible for data to be ported. However, this standard fee will be difficult to apply for medical history/ information especially if patient is part of research study.

- The time period would be better if it is similar to the time frame set for access obligation where it's stated that 'If the organisation is unable to comply with the requirement within 30 calendar days from the time it receives the request, it must inform the individual of when it will respond to the request within that time'.

- There should always be provisions for the organisation to give grounds for failure, non-compliance and for the organisation to rectify and re-transmit, rather than immediate levying of penalties, unless there is clear evidence of gross negligence on the part of the organisation.

- It may also not fair for data that has been costly collated be ported over for almost free (e.g. pathology tests, DNA sequencing), especially if "small companies" provides incentives (vouchers, free medical check up, money?) to the patient for valuable data to be ported over to them.

<u>Clarifications required:</u>

i. *Who sits on PDPC? Does it comprise of lay people from various sectors of society, similar to how our human and animal research ethical boards reviewing research protocols?*

ii. *Who audits/ oversees PDPC for the reviews done?*

iii. *At what level of detail should data be ported? Even when the individual specifically requests certain data to be ported, it will take a long time for these data to be collated, especially if this individual is involved in research as subjects.*
    - *If patient is part of a study and had his/her samples analysed, diagnosed, his DNA sequenced and so on, is the Institution under obligation to transfer these sets of data to the other Institution at Patient's request?*
    - *How will these data be given to the other party?*
        - *In raw form or structured?*

- *If in raw form, how will the receiving Institution make sense of it?*
- *If it's in a structured form, will it include comments/ assessments/ diagnosis from the originating Institution?*
- *If assessments are incorrect/ incomplete, will this potentially raise Legal issue?*
- *Will this create unnecessary stress to the health providers by carefully filling the data in the system?*

iv. If there is data leak, how would one determine or proof where the leak originates?

Q6. What are your views on the proposed binding codes of practices that set out specific requirements and standards for the porting of data in specific clusters or sectors?

- It is good that binding codes of practice are set out in specific clusters or sectors since
  - data collected by various clusters/ sectors may differ
  - some data may be sensitive and/ or confidential and if shared may harm the competitive position of the organisation.

- This is an opportunity to standardise the formats of various information we share between healthcare providers and other parties which we routinely interact with (insurance companies, VWOs, etc).

- Should be determined through comprehensive and wide-ranging consultations.
  - E.g. policies and forms must be drawn up according to our document management and release workflow, and standardised across the cluster and data should be encrypted and protected as per PDPA guidelines.

- Should only be implemented only in sectors where data portability has potential for benefits.

- If they are too restrictive, it will lead to high compliance costs unless government funding will be made available to support the cluster/sector in adopting the binding codes.

- Unrealistic for PHIs to be able to ascertain the legitimacy of the receiving organisation.
  - PHIs should request for official consent from the patient for this transfer of data, and upon the patient's consent, transfer is processed.

- The onus should be on the patient to verify and confirm that the receiving organisation is legitimate and credible.

Proposed Data Innovation Provisions

Q7. What are your views on the proposed approach for organisations to use personal data for the specified businesses innovation purposes, without the requirement to notify and seek consent to use the personal data for these purpose?

- This will allow organisations to improve on their service to their clients and use personal data for specified business innovation purposes.

- The risks of negative impact to consumers from such initiatives are generally low.

- Should be included in our MOH PDPA Notification poster/brochure so that it would be easier to explain to patients or NOK when the query arises.

Q8. What are your views on the proposed definition of "derived data"?

- Require more clarification regarding the definition of derived data specific to the healthcare setting.
  - While there is some information that is clearly personal data that is provided or directly observed/measured from the individual, much of the information in our records have passed through some processing by a clinical staff member – would that be considered derived data?
  - Would all medical information derived from diagnostic tests or clinical analysis, and any other information not gotten from the patient be derived data?

- Derived data should belong to the organisation since resources were spent on deriving the data.

- If the data is going to be disclosed, it should not be able to identify the individual.

Q9. What are your views on the proposal for the Access, Correction and proposed Data Portability Obligations not to apply to derived personal data?

- Fair and reasonable and it protects the interests of the organisation that spent resources and effort to derive those data and for competitive edge against its competitors in terms of innovation.

Clarifications required:

i. *Who takes responsibility of wrong data when data is ported over?*

ii. *Do the "personal data" in these examples include "de-identified" data?*