PERSONAL DATA PROTECTION COMMISSION SINGAPORE

PRACTICAL GUIDANCE TO QUERIES BY MEDICAL RESEARCH INSTITUTION[1]

1 A Medical Research Institution (the "Institution") sought clarifications from the Personal Data Protection Commission (the "Commission") on two main issues: (i) the factors that Commission considers relevant in assessing what is "impracticable" under paragraph 2(b) of the Third Schedule[2] of the Personal Data Protection Act ("PDPA"); and (ii) whether the Commission is prepared to consider a process of de-identification of personal data, where the "key" to re-identification resides with another department within the institution with whom the research personnel or department would have no authority over, and appropriate policies, processes and safeguards are put in place to prevent re-identification by the research personnel or department. The Institution's queries relate to medical related research that falls outside the ambit of the Human Biomedical Research Act (No. 29 of 2015).

Assessing "impracticability" under paragraph 2(b) of the Third Schedule

2 When assessing whether it would be "impracticable" for an organisation to seek consent of the individual, the specific facts of the case will have to be considered.

3 Factors that the Commission considers relevant in assessing whether it is "impracticable" to seek consent may include, but are not limited to:

(a) The organisation does not have current contact information of the potential research subject nor sufficient information to seek up-to-date contact information. The organisation should be able to demonstrate that the potential research subject cannot be reached using the contact information, such as by attempting to contact the potential research subject;

(b) Given the target population required for meaningful conclusions to be drawn from the research, the quantum of the research grant and the period allotted for the research as a condition of the research grant, the financial, organisational costs of attempting to seek consent from each potential

[1] This document incorporates both the Practical Guidance, as well as the subsequent clarification provided on the Practical Guidance to the Medical Research Institution.

[2] Pursuant to paragraph 1(i) of the Third Schedule, an organisation may use personal data about an individual without consent of the individual where the personal data is used for a research purpose (including historical or statistical research) but only if the conditions in paragraph 2 of the Third Schedule are met. The conditions in paragraph 2 are as follows: (a) the research purpose cannot reasonably be accomplished unless the personal data is provided in an individually identifiable form; (b) it is impracticable for the organisation to seek the consent of the individual for the use; (c) the personal data will not be used to contact persons to ask them to participate in the research; and (d) linkage of the personal data to other information is not harmful to the individuals identified by the personal data and the benefits to be derived from the linkage are clearly in the public interest.

research subject would impose such disproportionate resource demands and burden on the institution or take up so much time (assuming the organisation has made every reasonable effort to provide for the required time and resources) that carrying out the research is no longer viable. In this regard, there is no fixed number of subjects that would be determined as "impracticable" to seek consent from. Such an assessment would be based on all relevant circumstances of the case, which may include the required number of research subjects, whether or not there is an existing relationship with the individuals, and other factors affecting the difficulty of contacting the required research subjects; and

(c) Exceptional circumstances where seeking the research subject's consent would affect the validity or defeat the purposes of the research, in particular, where seeking consent would skew the research or introduce bias into the research such that no meaningful conclusions can be drawn. Organisations should nevertheless consider whether it is possible to seek consent in a manner that would not introduce such bias.

4 To be clear, factors like mere inconvenience (to the organisation or the potential research subject), additional costs or time delays resulting from having to contact individuals for consent, on their own, are insufficient to demonstrate "impracticability". These, however, may be relevant considerations if the added financial or organisational costs (of having to seek consent from the individuals) is so onerous that the research is no longer viable. Organisations may wish to consider convenient and practical means for individuals to provide consent, for instance by replying to a letter, email, text message or recording of voice call, instead of requiring the individual to make a trip to the organisation's physical location for the purpose of giving consent.

5 The Commission would also highlight that where an organisation is using anonymised data, no personal data is used, therefore there is no need for the organisation to undertake activities to re-identify the individuals just for the purpose of seeking consent.

Relevance and/or impact of impracticability as determined by the Institutional Review Board ("IRB")

6 The Commission notes that in the course of conducting research, organisations may take into account the opinion of its IRB, or equivalent body, among other things, on whether it would be impracticable to seek the consent of individuals to use their personal data.

7 The Commission understands that the IRB comprises medical, scientific and/or non-scientific members who collectively possess the expertise and understanding of the types of research carried out by institutions, and whose role is to undertake independent review of research studies. In the event that the IRB has considered the issue of whether the circumstances in the specific case

renders it impracticable to seek the consent of the research subject, the Commission may consider the opinion of the IRB to represent the standard of conduct expected of a reasonable researcher. To be clear, the final decision lies with the Commission as the IRB cannot waive compliance with the PDPA.

Application of the PDPA to data that has been anonymised for use by one department and the "key" to re-identification resides with another department within the institution

8 For purposes of the PDPA, the Commission will consider data to be "anonymised"[3] (i.e. not personal data) if an individual cannot be identified from that data, whether by itself or combined with other information that the organisation has or is likely to have access. Applying de-identification techniques to personal data does not in itself mean that the data has been anonymised, especially if such data can be readily converted back to personal data. In general, where the data is anonymised, the Data Protection Provisions in Parts III to VI of the PDPA do not apply to the collection, use or disclosure of such data. If an organisation has access to other information that can re-identify the individuals (e.g. the organisation holds the "key" to re-identification), the dataset will not be treated as anonymised and will continue to be considered personal data to which the Data Protection Provisions in Parts III to VI of the PDPA will apply.

9 Notwithstanding this, the Commission recognises that anonymisation can be relevant to the safe use of data within an organisation where effective barriers are established to prevent re-identification from the data, including restricting access by a group (or groups) of users within the organisation to information held by the organisation that could re-identify an individual.

10 An example of such a barrier could be policies and procedures that effectively ensure that users of anonymised data within the organisation do not have access to other data or information that can re-identify the individuals from the anonymised data.

11 In circumstances where the data is used by a specific group (or groups) of users who do not have access to information that can re-identify the individuals, the risk of re-identification is assessed to be not significant, and the data will not in effect be used as personal data (e.g. the data will not be used to make a decision about, or otherwise used in a manner that has an impact on an identifiable individual), the Commission could consider it a use of anonymised data, to which the Data Protection Provisions in Parts III to IV of the PDPA do not apply. In addition, organisations should consider safeguards that can reduce the risks of

[3] The term "anonymised data" used in this document is with reference to the definition in Chapter 3 (Anonymisation) of the Advisory Guidelines on the PDPA for Selected Topics.

re-identification, such as putting in place governance frameworks and policies on the use of anonymised data, as well as processes and controls to ensure the proper handling and security of the dataset.

12 The group of data users should also be mindful of its subsequent actions vis-à-vis the data, to ensure the risk of re-identification is not thereby increased. For example, the risks of re-identification may be significant if there are any subsequent disclosures of the anonymised data or information relating to the anonymised data to persons outside of the group, including recipients in the same organisation that may have access to other information which can, when combined with the anonymised data, lead to the re-identification of individuals, especially where no effective controls are imposed on the recipients. Given that the organisation still has access to information that could re-identify individuals from the anonymised data, the organisation must ensure the robust anonymisation of the data before any further disclosure beyond the group (or groups) of users such that the risk of re-identification will not be significant (e.g. this may include further scrambling of the data).

13 The Commission does not prescribe the manner in which organisations anonymise their dataset. It would be for the organisations to assess which would be the most appropriate anonymisation technique to use in their specific circumstances, in order to comply with their obligations under the PDPA. As good practice, organisations should consider the possibility of factors beyond their control which may pose a challenge in keeping data anonymised. For more information on anonymisation, please refer to Chapter 3 (Anonymisation) of the Advisory Guidelines on the PDPA for Selected Topics.

14 It should also be noted that the PDPA's position does not affect any authority, right or obligation arising under any other law. Organisations should ensure that any action they take are also in compliance with other applicable laws.

END OF DOCUMENT