ADVISORY GUIDELINES FOR THE HEALTHCARE SECTOR

ISSUED 11 SEPTEMBER 2014
REVISED 28 MARCH 2017

TABLE OF CONTENTS

PART I

1 Introduction

1.1 These Guidelines should be read in conjunction with the document titled "Introduction to the Guidelines"[1], including the disclaimers set out therein.

1.2 Developed together with the Ministry of Health ("MOH"), these Guidelines aim to address the unique circumstances faced by the healthcare sector in complying with the Personal Data Protection Act 2012 ("PDPA").

[1] Available at http://www.pdpc.gov.sg/resources/advisory-guidelines.

PART II: APPLICATION OF THE DATA PROTECTION PROVISIONS TO SCENARIOS FACED IN THE HEALTHCARE SECTOR

The following sections and examples outline the application of some of the Data Protection Provisions in the PDPA. They address particular aspects of the PDPA, and are not meant to exhaustively address every obligation in the PDPA that would apply in that scenario. These sections and examples do not illustrate the application of the Do Not Call Provisions, which are addressed in Part III of these Guidelines.

2 The Consent, Purpose Limitation and Notification Obligations

2.1 The PDPA requires organisations to, among other things, notify an individual of the purposes for the collection, use and disclosure of personal data[2] of the individual and obtain his consent, unless any relevant exception[3] applies. In situations where an individual voluntarily provides his personal data to an organisation for a purpose, and it is reasonable that he would voluntarily provide the data, the individual is deemed to consent to the collection, use or disclosure of the personal data. If an individual gives, or is deemed to have given, consent to the disclosure of personal data about the individual by one organisation to another organisation for a particular purpose, the individual is deemed to consent to the collection, use or disclosure of the personal data for that particular purpose by that other organisation.

2.2 The following examples mainly focus on the application of these obligations, including situations where consent may be deemed, or where exceptions to the Consent Obligation may apply. Brief references may also be made to other obligations where appropriate, although not every obligation in the PDPA that could apply to the example may be addressed.

---

[2] Personal data is defined in the PDPA as "data, whether true or not, about an individual who can be identified – a) from that data; or b) from that data and other information to which the organisation has or is likely to have access". While some data may necessarily relate to an individual, other data may not, on its own, relate to an individual. Such data would not constitute personal data unless it is associated with, or made to relate to, a particular individual. Generic information that does not relate to a particular individual may also form part of an individual's personal data when combined with personal data or other information to enable an individual to be identified.

[3] Please refer to the Second (collection of personal data without consent), Third (use of personal data without consent) and Fourth (disclosure of personal data without consent) Schedules under the PDPA for exceptions which may apply.

2.3 **Example: Collecting personal data from patients seeking medical care**

John visits Healthcare Institution ABC for the first time. The nurse informs John that he has to register and hands him a registration form to fill out. John voluntarily fills out the form and provides his full name, address, NRIC number and mobile number.

Consent from John can be deemed for certain purposes

By voluntarily providing his personal data (including through presenting himself for medical examination), John may be deemed to have consented to the collection, use and disclosure of his personal data (including data derived from ensuing medical examinations and tests) by Healthcare Institution ABC for the purpose of his visit, including any medical care that is to be provided in relation to the visit.

Depending on the actual circumstances, this could include:

- any associated examinations or tests;
- follow-up consultations in relation to the purpose of his visit to Healthcare Institution ABC; and
- the convening of a case conference with other doctors within Healthcare Institution ABC solely for the purpose of discussing treatment options for John.

There is likely to be deemed consent if Healthcare Institution ABC ensures that John was aware of the purposes for which his personal data would be collected, used or disclosed and it is reasonable that he would voluntarily provide his personal data for such purposes.

Whether deemed consent would cover purposes beyond the provision of medical care to John

Deemed consent does not cover purposes outside those for which the personal data was provided. If Healthcare Institution ABC intends to use or disclose such personal data beyond the purpose of John's visit and in particular for purposes that are not related to provision of medical care, it is less likely to be covered by deemed consent and in such instances Healthcare Institution ABC should notify John of such purposes and obtain his consent.

For example, Healthcare Institution ABC may wish to use John's personal data for marketing of health products unrelated to John's condition. It is unlikely that John would be deemed to have given his consent for this purpose, since such usage has

	no nexus to his visit to Healthcare Institution ABC or the provision of medical care related to his visit. In this case, Healthcare Institution ABC should notify John of such purposes and obtain his consent. <u>Other considerations</u> *Consent cannot be required beyond what is reasonable to provide the service* In deciding what personal data to collect from patients, Healthcare Institution ABC should note that section 14(2)(a) of the PDPA provides that an organisation providing a product or service to an individual must not, as a condition of providing the product or service, require the individual to consent to the collection, use or disclosure of his personal data beyond what is reasonable to provide the product or service. As good practice, Healthcare Institution ABC should not collect more personal data than is required for its business or legal purposes. It is also good practice for Healthcare Institution ABC to indicate which fields in the form that collect personal data are compulsory and which are optional. *How the Retention Limitation Obligation applies* Healthcare Institution ABC may retain John's personal data after John's visit is completed, if there is a legal or business purpose to do so. For example, Healthcare Institution ABC may retain John's personal data in accordance with regulation 12 of the Private Hospitals and Medical Clinics ("PHMC") Regulations (which, in brief, provides that licensed healthcare institutions must maintain medical records for such periods as may be required by the Director of Medical Services).
2.4	**Obtaining consent from patients for medical students or doctors on an attachment programme to collect, use and disclose their personal data as part of providing medical care** John visits Healthcare Institution ABC to seek medical care. As illustrated in the example above, John may be deemed to have consented to the collection, use and disclosure of his personal data by Healthcare Institution ABC for the purpose of his visit (including the medical care that is to be provided in relation to the purpose of his visit) by voluntarily providing his personal data (including through presenting himself for medical examination). The consent deemed to have been provided from John will cover all activities which Healthcare Institution ABC (including employees and volunteers) has to undertake for the purpose of John's visit. The employees and volunteers involved in John's care at Healthcare Institution ABC would not need to obtain separate consent from John to collect, use or disclose his personal data for the purpose of providing

	medical care to him. Depending on the actual circumstances, the employees and volunteers could include doctors or medical students providing medical care as part of a formal attachment programme with Healthcare Institution ABC. An 'employee' under the PDPA includes a volunteer working under an unpaid volunteer work relationship.
2.5	**Example: Disclosing personal data in referral cases** During separate consultations with the following patients, a doctor makes the recommendations as follows: a) for Patient A to consult a specialist; b) for Patient B to visit a hospital for further medical tests; and c) for Patient C to consider long term care services at a nursing home. Patients A, B and C each agree (verbally) to the respective recommendations and the doctor proceeds to make the necessary arrangements, for example, by contacting another doctor directly or providing the patient with a referral letter[4]. Since each patient agreed to the recommendation, he would have consented to the doctor disclosing his personal data as required for the referral when contacting the recommended healthcare service provider directly. In cases where the doctor provides the patient with the referral letter, and the patient takes the referral letter to the organisation he is being referred to, it is the patient who would be considered to have disclosed his personal data to that organisation. As good practice, the doctor could consider documenting a verbal consent given, such as by making a note in the patient's file. Having evidence supporting verbal consent would be useful in the event of a dispute. Before the doctor discloses Patients A, B and C's personal data to these organisations, he should take reasonable steps to ensure that their personal data is accurate and complete (in compliance with the PDPA's Accuracy Obligation, the PHMC Act and the regulations made thereunder, and the Singapore Medical Council Ethical Code and Ethical Guidelines, as may be applicable).

[4] Generally speaking, the PDPA obligations are not affected by whether the letter is addressed to a specified doctor or an unspecified doctor.

	For the avoidance of doubt, the doctor may disclose the personal data pursuant to such consent regardless of whether or when Patients A, B and C arrive at the respective facility to which they have been referred.
2.6	**Example: Collecting personal data of other individuals from a patient for medical care** During John's consultation, the doctor asks if John has had any family history of cancer, as it is relevant to provide medical care to John. John informs the doctor that his Aunt Kim has had stomach cancer. This may or may not be considered personal data of Aunt Kim, depending on whether Aunt Kim can be identified by the organisation that is collecting such data (through the doctor) from this data itself or when this data is combined with other likely accessible data or information. <u>If Aunt Kim can be identified</u> The doctor asks John for more details about Aunt Kim including her medical history, like her full name and the healthcare institution she sought treatment at, as the information is relevant to provide medical care to John. In this case, the doctor is likely to be collecting personal data about Aunt Kim. The organisation (through the doctor) may collect the personal data of Aunt Kim without her consent under an exception provided in paragraph 1(m) of the Second Schedule to the PDPA[5], as the personal data was provided to the organisation (through the doctor), by another individual (John), to enable the organisation to provide a service for the personal and domestic purposes of that other individual (medical care for John). If the organisation wishes to use or disclose Aunt Kim's personal data without her consent for purposes consistent with the purpose of the collection, it may do so pursuant to the exceptions provided in paragraph 1(j) of the Third Schedule and 1(s) of the Fourth Schedule respectively[6]. The organisation is still obliged to comply with the other Data Protection Provisions in the PDPA, such as the obligation to protect Aunt Kim's personal data.

[5] Under paragraph 1(m) of the Second Schedule, an organisation may collect personal data about an individual without the consent of the individual or from a source other than the individual where the personal data was provided to the organisation by another individual to enable the organisation to provide a service for the personal or domestic purposes of that other individual.

[6] Generally, paragraphs 1(j) of the Third Schedule and 1(s) of the Fourth Schedule allow organisations to use or disclose personal data collected without consent in accordance with the Second Schedule, for purposes consistent with the original purpose of collection. Please refer to the PDPA for more information.

	If Aunt Kim cannot be identified The doctor does not ask John for more details about Aunt Kim, as he determines that it is not relevant to provide medical care to John. If the organisation that is collecting the data (through the doctor) cannot identify Aunt Kim from this data (or when combining this data with other likely accessible data or information), then the data is not personal data and the PDPA does not apply.
2.7	**Example: Collecting, using or disclosing personal data for purposes other than for the patient's visit or medical care** Clinic/ Healthcare Institution ABC ("Health Organisation ABC") wishes to collect, use or disclose John's personal data when he visits the clinic for medical care and the following purposes: a) review of internal processes for quality assurance, service improvement and corporate business functions; and b) formulation of teaching material, e.g. as part of a case study, lecture slides or other types of teaching material used for teaching purposes. Generally, Health Organisation ABC should notify John of its intended purposes and obtain his consent for such purposes, unless any relevant exception applies. Health Organisation ABC is free to determine the appropriate means by which it notifies and obtain consent from John. In relation to the specific purposes above: a) For internal quality assurance, service improvement, and corporate business functions: Health Organisation ABC is unlikely to be required to specifically notify John of such internal corporate purposes that support the delivery of medical care to him and/or obtain consent for them[7]; and b) For formulation of teaching material: Health Organisation ABC should typically notify John of such purposes and obtain consent if the data cannot be anonymised.

[7] An organisation need not specify every activity it will undertake in relation to collecting, using or disclosing personal data when notifying individuals of its purposes. Purposes should be stated at an appropriate level of detail for the individual to determine the reasons for which the organisation will be collecting, using or disclosing his personal data. Please refer to Chapter 14 of the Advisory Guidelines on Key Concepts in the PDPA for more information.

	Consent from patients would not be required where the training or professional registration activities do not involve the collection, use or disclosure of their personal data. (E.g. where a trainee doctor records in his log-book or reports only information that does not contain personal data of patients, such as the number of hours he has spent performing a particular medical procedure or other information that does not identify any patient[8].) Organisations should also note that the Data Protection Provisions would not affect any regulatory requirements by or under the laws which govern professional training or registration requirements for doctors and other healthcare professionals. (E.g. under the Medical Registration Act, certain conditions may be imposed by the Singapore Medical Council in respect of the registration of provisionally registered doctors.) <u>Cannot require consent for additional purposes unless reasonably required to provide medical care</u> If these additional purposes are not reasonably required to provide John with the service of medical care, Health Organisation ABC cannot require John to consent to his personal data being used for these purposes as a condition of providing him the medical care service (section 14(2)(a) of the PDPA). <u>Other considerations</u> As good practice, Health Organisation ABC should consider if it is able to achieve the same purposes without using personal data. For example, using anonymised datasets that do not relate to any identifiable individual. Health Organisation ABC will not need to obtain consent from individuals if the personal data in its possession is anonymised before use. Consent is also not required if Health Organisation ABC uses and discloses the anonymised data[9]. If Health Organisation ABC intends to send a specified message to John's Singapore telephone number (e.g. to advertise a service provided by ABC), then the Do Not Call Provisions will apply (addressed in Part III below).

[8] The patient should not be identifiable whether from that data itself or together with other information that the organisation has or is likely to have access to.

[9] Although an organisation may consider a data set anonymised, it should consider the risk of re-identification if it intends to publish or disclose the data set to another organisation. Please refer to the chapter on "Anonymisation" in the Advisory Guidelines on the PDPA for Selected Topics for more information on the issue of re-identification.

2.8	**Example: Collecting personal data of individuals to respond to an emergency** John takes his father to Clinic ABC. His father has been suffering from a very high fever for a few days. During the doctor's examination, John's father suddenly collapses. Clinic ABC immediately calls an ambulance to transfer him to a hospital. This involves Clinic ABC disclosing John's father's personal data to the hospital and ambulance services. Clinic ABC and the hospital may collect, use and disclose John's father's personal data without consent to respond to an emergency that threatens his life or health. This is pursuant to the exceptions in paragraph 1(b) of the Second Schedule, paragraph 1(b) of the Third Schedule and paragraph 1(b) of the Fourth Schedule of the PDPA[10].
2.9	**Example: Disclosing personal data of individuals to managed care providers or employers** John visits Clinic ABC, one of the clinics registered under his company's healthcare scheme. The healthcare scheme is managed by Organisation XYZ, a managed care provider. Clinic ABC receives several calls asking for information relating to John's visits to the clinic: a) John's employer asks the clinic for the number of times John has visited the clinic and the medical conditions he has been diagnosed with, for its own purposes. b) Organisation XYZ asks the clinic for the number of times John has visited the clinic and the medical conditions he has been diagnosed with, (i) for its own purposes or (ii) for John's employer. Clinic ABC may only disclose John's personal data with his consent or if any relevant exception under the PDPA applies. In considering whether it should disclose John's personal data to his employer or the managed care provider, in addition to its PDPA obligations, Clinic ABC should

[10] Under paragraphs 1(b) of the Second, Third and Fourth Schedules, an organisation may collect, use or disclose (as the case may be) personal data about an individual without the consent of the individual or from a source other than the individual where the collection, use or disclosure (as the case may be) is necessary to respond to an emergency that threatens the life, health or safety of the individual or another individual.

	give careful consideration to whether such disclosure would be in breach of other legal obligations[11] and ethical requirements.
2.10	**Example: Consent given for a purpose will cover activities undertaken for that purpose** Before collecting, using or disclosing personal data, organisations must notify individuals of their purposes and obtain consent unless any exception in the PDPA applies. However, when specifying its purposes relating to personal data, an organisation is not required to specify every activity which it may undertake, but rather its objectives or reasons for the collection, use or disclosure (as the case may be) of the personal data. Healthcare Institution XYZ maintains its patients' medical records on a national health records database. Healthcare Institution XYZ has obtained John's consent for the collection, use and disclosure (to other healthcare institutions) of his personal data for the purpose of providing medical treatment to him. Healthcare Institution XYZ is not required to separately obtain John's consent to maintain his medical records on the database, or to disclose the relevant records to other healthcare institutions through the database, if such activities are undertaken for the purpose that John has consented to.
2.11	**Example: Consent obligation imposed on organisations, not on employees** Doctor Mei Ling is the sole proprietor of Clinic ABC. Doctor Mei Ling: a) Employs Doctor Hussein as the second doctor at Clinic ABC. b) Engages Doctor Ravi as a locum doctor to stand in at the clinic when she is on holiday. Doctor Hussein is an employee of Clinic ABC. The PDPA provides that the Data Protection Provisions do not impose any obligations on any employee acting in the course of his or her employment with an organisation. Any act done or conduct engaged in by a person in the course of his employment will be treated as done or engaged in by his employer for purposes of the PDPA[12]. Hence, Clinic ABC will have

[11] Please refer to Chapter 5 below on Rights and obligations, etc under other laws.

[12] Section 53 of the PDPA provides that:

	to ensure compliance with the Consent Obligation in respect of the collection, use and disclosure of personal data by Doctor Hussein, unless any relevant exception applies. The specific Data Protection Provisions relevant for the locum doctor Doctor Ravi will depend, among other things, on the arrangements between Doctor Ravi and Clinic ABC, such as whether Doctor Ravi is processing personal data for the purposes of Clinic ABC pursuant to a written contract[13] or whether Doctor Ravi was engaged as an employee of Clinic ABC. If Doctor Ravi is not an employee of Clinic ABC, the exclusion for employees will not apply to him and he may thus be subject to the Data Protection Provisions. If, however, Clinic ABC engages Doctor Ravi as an employee, then Clinic ABC will have to ensure compliance with the Consent Obligation in respect of the collection, use and disclosure of personal data by Doctor Ravi, unless any relevant exception applies. Doctor Mei Ling should ensure that Clinic ABC's contractual arrangements with Dr Hussein and Dr Ravi are consistent with the Data Protection Provisions in the PDPA and any other applicable legislation.
2.12	**Example: Acquisition of medical practice by another organisation** Doctor Mei Ling has been the sole proprietor of Clinic ABC. She retires and transfers her business to Doctor Hussein. She wants to give him access to all of her patients' personal data. In this scenario, paragraph 1(p) of the Second Schedule and paragraph 1(p) of the Fourth Schedule relating to business asset transactions could apply (subject to the

(1) Any act done or conduct engaged in by a person in the course of his employment (referred to in this section as the employee) shall be treated for the purposes of this Act as done or engaged in by his employer as well as by him, whether or not it was done or engaged in with the employer's knowledge or approval.

(2) In any proceedings for an offence under this Act brought against any person in respect of an act or conduct alleged to have been done or engaged in, as the case may be, by an employee of that person, it is a defence for that person to prove that he took such steps as were practicable to prevent the employee from doing the act or engaging in the conduct, or from doing or engaging in, in the course of his employment, acts or conduct, as the case may be, of that description.

[13] Section 4(2) of the PDPA provides that Parts III to VI (except for section 24 (protection of personal data) and section 25 (retention of personal data)) shall not impose any obligation on a data intermediary in respect of its processing of personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing. Please refer to the section on data intermediaries below for more information.

	conditions in paragraph 3 of the Second Schedule and paragraph 3 of the Fourth Schedule respectively). Paragraph 1(p) of the Second Schedule allows Doctor Hussein to collect personal data about Doctor Mei Ling's patients without consent, as a party to a business asset transaction (the business transfer) with Doctor Mei Ling, to the extent that personal data collected relates directly to the part of the organisation or its business assets with which the business asset transaction is concerned. The corresponding paragraph 1(p) of the Fourth Schedule allows Doctor Mei Ling to disclose personal data about her patients to Doctor Hussein without consent.
2.13	**Example: Using personal data for a research purpose without consent** Health Organisation ABC wishes to conduct retrospective research studies using medical records of individuals collected many years ago from its various patient databases, including both its research and administrative databases. The purpose of this research is to gain a better understanding of the epidemiology of diseases and socio-demographic characteristics of past patients which would influence ABC's public health strategies. The research purpose cannot reasonably be accomplished unless the personal data is provided in an individually identifiable form. Health Organisation ABC did not retain the contact information of those individuals and has no knowledge of whether these patients have passed away or have relocated to another country. Hence it would be impracticable for Health Organisation ABC to seek consent from the individuals for the use. Health Organisation ABC has no intention of contacting these patients to ask them to participate in the research. In addition, 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. In this case, Health Organisation ABC is likely to be able to use personal data about these individuals without consent, pursuant to the paragraph 1(i) exception in the Third Schedule of the PDPA for research purposes. In determining if it would be impracticable to seek the consent of these individuals, Health Organisation ABC may wish take into account the opinion of its Institutional Review Board ("IRB"), or equivalent body, which provides ethics approval for research projects.

Organisations and Data Intermediaries

2.14 In some situations, healthcare institutions may engage data intermediaries to process personal data. The PDPA provides that a data intermediary[14] that processes personal data on behalf of and for the purposes of another organisation pursuant to a contract which is evidenced or made in writing will only be subject to the Protection Obligation and Retention Limitation Obligation and not any of the other Data Protection Provisions.

2.15 A data intermediary remains responsible for complying with all Data Protection Provisions in respect of other activities that do not constitute processing of personal data on behalf of and for the purposes of another organisation that is pursuant to a contract evidenced or made in writing.

2.16 In any case, under section 4(3) of the PDPA, the organisation that engages the data intermediary would still have the same obligations under the PDPA in respect of personal data processed on its behalf as if the personal data were processed by the organisation itself.

2.17 Please refer to the Advisory Guidelines on Key Concepts in the PDPA which provide further elaboration on when an organisation is considered a data intermediary and the obligations applicable to data intermediaries under the PDPA.

2.18	**Example: Provision of laboratory testing services** Clinic ABC has a written contract with an external vendor, Lab 123 for the provision of blood testing services to ABC's patients who require it. Among other things, the contract between Clinic ABC and Lab 123 specifies that Lab 123 will use personal data of Clinic ABC's patients provided by Clinic ABC for the sole purpose of conducting the blood test on behalf of and for the purposes of Clinic ABC. John visits Clinic ABC and the doctor determines that a blood test is required for his medical care. John agrees verbally to the blood test, and allows the doctor to draw his blood[15]. Clinic ABC provides John's personal data to Lab 123 for the purposes of the blood test.

[14] PDPA defines data intermediary as "an organisation which processes personal data on behalf of another organisation but does not include an employee of that other organisation".

[15] In this case, John would be considered to have provided consent to Clinic ABC for the collection, use and disclosure of his personal data for the purpose of the blood test.

	In this case, Lab 123 would be considered a data intermediary processing John's personal data on behalf of and for the purposes of Clinic ABC pursuant to a written contract in relation to conducting John's blood test. Lab 123 will be subject only to the Protection Obligation and the Retention Limitation Obligation, while Clinic ABC will have the same obligations under the PDPA in respect of John's personal data processed on its behalf by Lab 123, as if the personal data were processed by Clinic ABC itself.

3 The Access and Correction Obligations

Requirement to provide access to personal data ("Access Obligation")

3.1 Section 21(1) of the PDPA provides that, upon request by an individual, an organisation shall provide the individual with the following as soon as reasonably possible:

a) personal data about the individual that is in the possession or under the control of the organisation; and

b) information about the ways in which that personal data has been or may have been used or disclosed by the organisation within a year before the date of the individual's request.

Exceptions to the Access Obligation

3.2 The obligation in section 21(1) is subject to a number of exceptions in section 21(2) to (4) including some mandatory exceptions relating to situations where an organisation must not provide access.

3.3 Section 21(2) of the PDPA provides that an organisation is not required to provide individuals with the personal data or other information in respect of the matters specified in the Fifth Schedule to the PDPA. One example is where the personal data in question is opinion data kept solely for an evaluative purpose (paragraph 1(a) in the Fifth Schedule).

3.4 Section 21(3) specifies a number of situations in which an organisation must not provide access to personal data or other information. These include situations where providing access could reasonably be expected to cause immediate or grave harm to the safety or to the physical or mental health of the individual who made the request, or reveal the identity of the individual who provided the personal data and that individual does not consent to the disclosure of his identity[16].

Where the access request relates to legal proceedings

3.5 Where the individual who makes an access request for personal data is concurrently engaged in legal proceedings with the organisation, the organisation would not be required to provide the requested personal data if a relevant exception under the PDPA applies. One possible exception is in paragraph 1(h) of the Fifth Schedule. This exception provides that an organisation is not required to provide access to personal data collected, used or disclosed without consent (under exceptions that are

[16] Please refer to the PDPA for the full set of exceptions.

provided for in the PDPA)[17] for the purposes of an investigation if the investigation and associated proceedings and appeals have not been completed.

3.6 Organisations should note that all the Data Protection Provisions of the PDPA do not affect discovery obligations under law that parties to a legal dispute may have (e.g. pursuant to any order of court).

Requirement to correct personal data ("the Correction Obligation")

3.7 Section 22(1) of the PDPA provides that an individual may submit a request for an organisation to correct an error or omission in the individual's personal data that is in the possession or under the control of the organisation (a "correction request"). Upon receipt of a correction request, the organisation is required to consider whether the correction should be made.

3.8 In particular, section 22(2) goes on to provide that unless the organisation is satisfied on reasonable grounds that the correction should not be made, it should –

a) correct the personal data as soon as practicable; and

b) send the corrected personal data to every other organisation to which the personal data was disclosed by the organisation within a year before the date the correction request was made, unless that other organisation does not need the corrected personal data for any legal or business purpose.

3.9 If an organisation is satisfied upon reasonable grounds that a correction should not be made (whether the organisation is responding to a correction request made directly by the individual or has been notified of a correction made by such an organisation), section 22(5) requires the organisation to annotate (that is, make a note to) the personal data in its possession or under its control indicating the correction that was requested but not made. As good practice, the organisation may also wish to annotate the reasons why it has decided that the correction should not be made.

3.10 The obligation to correct personal data is subject to a number of exceptions in section 22 and the Sixth Schedule of the PDPA. Section 22(6) provides that an organisation shall not be required to correct or otherwise alter an opinion, including a professional or an expert opinion. One such exception in the Sixth Schedule relates to personal

[17] This exception applies in respect of personal data that was collected, used or disclosed without consent, under paragraph 1(e) of the Second Schedule, paragraph 1(e) of the Third Schedule or paragraph 1(f) of the Fourth Schedule, respectively.

data which is opinion data kept solely for an evaluative purpose as defined under the PDPA[18].

3.11 The following examples illustrate the application of the Access and Correction Obligations.

3.12	**Example: Responding to requests to access personal data** John makes an access request to Clinic ABC, requesting for access to his personal data and how it has been used and disclosed by the clinic, on 5th December 2015. Clinic ABC has to provide John with the complete set of personal data requested that is in its possession or under its control (e.g. including personal data contained in its files in storage), and inform him about the ways in which the personal data has been or may have been used or disclosed, subject to any relevant exceptions in the PDPA. The clinic may, in good faith, ask John to be more specific as to what personal data he requires, to facilitate processing of the access request, or to determine whether the request falls within one of the exceptions in the Fifth Schedule to the PDPA. Before responding to an access request, the clinic should exercise due diligence and adopt appropriate measures to verify John's identity. <u>How the personal data should be provided</u> The clinic is not necessarily obliged to provide John with copies of the original documents in which the requested personal data reside (e.g. registration forms or doctor's notes) although it may be the most convenient means to provide access. Where possible, the clinic may provide such personal data in a form other than the original form in which such personal data was recorded. *Example 1* John requests access to personal data that he had provided through a registration form. In addition to the registration form, the clinic had recorded the personal data in a patient record card, and in an electronic system. The clinic is required to provide John with all his personal data but is not required to provide a duplicate of the registration form, patient record card or electronic system.

[18] Please refer to the PDPA for the full set of exceptions.

	Example 2 John requests for the diagnosis of a condition that he had visited the clinic for, which had been recorded in handwritten notes of the doctor. The clinic is not obliged to provide a photocopy of the handwritten notes, although it should provide John with the information he requested in an appropriate form, such as through a medical report, unless a relevant exception applies. <u>Providing information about how personal data has been used and disclosed</u> In relation to how the personal data has been used and disclosed, the clinic has to provide John with information about the ways in which his personal data has been or may have been used or disclosed within a year before the date of request, i.e. for the period 6th December 2014 to 5th December 2015, unless any exception applies. The clinic may develop a standard list of parties to which personal data is routinely used and disclosed, and in many cases, may provide this standard list as the first response to access requests for information relating to how the personal data has been or may have been disclosed within the past year. The clinic should keep this list updated. <u>Other matters relating to an access request</u> The clinic may charge John a reasonable fee for the access request, and must respond to the access request as soon as reasonably possible. If the clinic is unable to respond to an access request within 30 days from the time the request is made, the clinic must inform John in writing within the 30 day time frame of when it will be able to respond to the request, which should be the soonest possible time it can provide access. More information on how an organisation should respond to an access request and what constitutes a 'reasonable fee' can be found in Chapter 15 of the Advisory Guidelines on Key Concepts in the PDPA.
3.13	**Example: Responding to requests for correction of personal data** John makes the following requests to Clinic ABC: a) To correct his contact details in the clinic's records to reflect his new postal address. b) To correct the information about his smoking habits which the doctor recorded during a visit by him to the clinic. c) To correct a diagnosis about his medical condition.

	In relation to the scenarios above, a) It would be reasonable for Clinic ABC to correct John's contact details to ensure that they are accurate and current. b) The clinic may decide not to correct its record about John's smoking habits, if it is satisfied upon reasonable grounds that a correction need not be made. c) Where the diagnosis is a professional or expert opinion, section 22(6) of the PDPA provides that the clinic is not required to correct or otherwise alter it. If the clinic does not make the corrections requested, the clinic should annotate such personal data with the corrections that were requested but not made.

4 The Protection, Accuracy, Retention Limitation, Transfer Limitation and Openness Obligations

4.1 The Advisory Guidelines on Key Concepts in the PDPA elaborates on these obligations. Like other organisations, healthcare institutions should consider the application of these obligations to their specific contexts.

4.2 In relation to the Protection Obligation, the PDPA requires an organisation to make reasonable security arrangements to protect personal data in its possession or under its control. There is no 'one size fits all' solution for organisations to comply with the Protection Obligation. Generally, where the personal data stored is regarded as more confidential and where the adverse impact to individuals is significantly greater if such personal data were inadvertently accessed (e.g. relating to sensitive medical conditions), tighter security arrangements should be employed. Healthcare institutions should consider the nature of the personal data in their possession or under their control (as the case may be) to determine the security arrangements that are reasonable and appropriate in the circumstances.

4.3 In relation to the retention of patient files and records, section 25 of the PDPA requires an organisation to 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 the purpose for which that personal data was collected is no longer being served by retention of the personal data, and retention is no longer necessary for legal or business purposes. Generally speaking, retaining personal data of existing patients for the purpose of having access to their consultation history would be considered a business purpose. It should be noted that the PDPA does not require an organisation to delete all personal data about the individual concerned upon receipt of a notice withdrawing consent.

4.4 The PDPA does not prescribe a specific retention period for personal data. However, healthcare institutions should review the personal data it holds on a regular basis to determine if that personal data is still needed. Healthcare institutions should not keep personal data "just in case", when it is no longer necessary for the purposes for which the personal data was collected or for any legal or business purpose. Attention is drawn to Regulation 12(3) of the PHMC Regulations and the MOH's *2015 Guidelines for the Retention Periods of Medical Records*.

5 Rights and obligations, etc under other laws

Existing rights, etc under law and other written law

5.1 Section 4(6)(a) of the PDPA states that unless otherwise provided in the PDPA, nothing in Parts III to VI of the PDPA (the Data Protection Provisions in the PDPA) shall affect any authority, right, privilege or immunity conferred, or obligation or limitation imposed, by or under the law, including legal privilege, except that the performance of a contractual obligation shall not be an excuse for contravening the PDPA.

5.2 Section 4(6)(b) states that the provisions of other written law shall prevail to the extent that any provision of Parts III to VI is inconsistent with the provisions of that other written law. That is, the provisions of the other written law will apply in respect of the matter(s) which is inconsistent between those provisions and Parts III to VI of the PDPA. Other provisions in the PDPA which are not inconsistent with the other written law will continue to apply. Accordingly, organisations should continue to comply with their obligations under other written laws such as the PHMC Act, National Registry of Diseases Act, Infectious Diseases Act, and Advance Medical Directive Act.

5.3 Section 13(b) of the PDPA provides that an organisation shall not, on or after the Data Protection Provisions come into effect, collect, use or disclose personal data about an individual without the consent of the individual unless the collection, use or disclosure, as the case may be, without the consent of the individual is required or authorised under the PDPA or any other written law.

5.4	**Example: Requirement to comply with other written law** Section 6(1) of the Infectious Diseases Act (Cap. 137) states that every medical practitioner who has reason to believe or suspect that any person attended or treated by him is suffering from an infectious disease or is a carrier of that disease shall notify the Director of Medical Services within the prescribed time and in such form or manner as the Director may require. As this is a requirement under written law, the medical practitioner is not required under the PDPA to obtain the consent of the individual in order to notify the Director in compliance with the Infectious Diseases Act.

Use of personal data collected before the appointed day

5.5 Section 19 of the PDPA provides that notwithstanding the other provisions of Part IV of the PDPA (which relate to collection, use and disclosure of personal data), an organisation may use personal data collected before the appointed day (i.e. 2nd July 2014) for the purposes for which the personal data was collected, unless consent for such use is withdrawn or the individual has indicated to the organisation that he does not consent to the use of the personal data. Such 'use' could include disclosure that is necessarily part of the organisation's use of such personal data.

5.6 The effect of section 19 is that organisations can continue to use personal data collected before the appointed day for the same purposes for which the personal data was collected without obtaining fresh consent, unless the individual has withdrawn consent (whether before on, or after the appointed day).

5.7 For the avoidance of doubt, the Do Not Call Provisions will apply to the sending of specified messages to Singapore telephone numbers, even if the Singapore telephone numbers had been collected before the appointed day.

5.8	**Example: Using personal data collected before the appointed day** Dental Clinic ABC collected John's personal data before 2nd July 2014 and has been sending him reminders by post to visit the dental clinic. Hitherto, John has not withdrawn consent nor has he indicated that he does not consent to such use of his personal data. Dental Clinic ABC may continue to send such reminders to John until he indicates that he no longer wishes to receive them.

PART III: APPLICATION OF THE DO NOT CALL PROVISIONS TO SCENARIOS FACED IN THE HEALTHCARE SECTOR

The following sections and examples set out the application of the Do Not Call Provisions and the Personal Data Protection (Exemption from Section 43) Order (S 817/2013) ("Exemption Order") to scenarios faced in the healthcare sector. They are not meant to exhaustively address every obligation in the PDPA that would apply in that scenario. In particular, they do not illustrate the application of the Data Protection Provisions, which were addressed earlier in these Guidelines.

6 The Do Not Call Provisions

6.1 Messages with a purpose to offer to supply, advertise or promote goods or services, land or an interest in land, or a business or investment opportunity, or a supplier of such goods, services, land or opportunity are specified messages[19] and the Do Not Call Provisions will apply to such messages. Messages which do not contain any of such purposes would not be considered specified messages.

6.2 In addition, some types of messages, listed in the Eighth Schedule, are excluded from the definition of a specified message. Some examples include:

a) "business-to-business" marketing messages;

b) any message sent by a public agency under, or to promote, any programme carried out by any public agency, which is not for commercial purpose;

c) any message the sole purpose of which is to facilitate, complete or confirm a transaction that the recipient of the message has previously agreed to enter into with the sender; and

d) any message the sole purpose of which is to conduct market research or market survey.

6.3 The Do Not Call Provisions apply to a specified message addressed to a Singapore telephone number if the sender of the specified message is present in Singapore when the specified message is sent or the recipient of the specified message is present in Singapore when the specified message is accessed.

[19] Please refer to section 37 of the PDPA for the full definition of a specified message (including the Eighth Schedule for the list of exclusions from the definition of specified message).

6.4	**Example: Messages that are not specified messages** *Example 1* Clinic ABC calls John at his Singapore telephone number on different occasions solely for one of the following purposes: a) To confirm that he has completed the full course of his medication. b) To check that his fever has subsided. c) To make an appointment to review the results from the previous check up. These messages are unlikely to be considered specified messages. *Example 2* James visits Dental Clinic DEF for the first time for a dental treatment. At the end of the visit, James makes an appointment with Dental Clinic DEF for his next visit. A week before the appointment date, Dental Clinic DEF sends James a text message at his Singapore telephone number solely to remind him of his appointment. Such a reminder sent by Dental Clinic DEF solely for the purpose of reminding James of his appointment would unlikely be considered a specified message.

6.5 One significant obligation under the Do Not Call Provisions is that the organisation sending the specified message will have to check with the Do Not Call Registry, unless:

a) the user or subscriber of the Singapore telephone number has given clear and unambiguous consent in written or other accessible form to the sending of the specified message to that number; or

b) the organisation is exempted from complying with its obligation under the Exemption Order.

6.6	**Example: Obtaining clear and unambiguous consent** *Example 1* Clinic ABC sends out a letter to inform all its former patients about a new healthcare supplement. The letter says that unless they reply to opt out, they would be

	considered to have provided consent for Clinic ABC to call them to market the supplement. Peter does not reply to opt out. The failure to opt out by Peter is in itself unlikely to constitute clear and unambiguous consent for Clinic ABC to call him for purposes of marketing the supplement. Clinic ABC must check the DNC Register and receive confirmation that Peter's number is not listed before calling him to market the supplement. *Example 2* Jason visits Dental Clinic DEF for the first time for a dental treatment. When providing his personal data to Dental Clinic DEF in the patient registration form, Jason checks a box to indicate that he consents to receiving reminder text messages from Dental Clinic DEF for subsequent dental visits. Jason would be considered to have provided clear and unambiguous consent for Dental Clinic DEF to send reminder text messages for his next dental visits. Dental Clinic DEF may send such messages to Jason without checking the Do Not Call Registry.

Exemption Order

6.7 The Exemption Order allows organisations to send a text or fax message (but not voice call) on similar or related products, services and memberships to individuals with whom they have an ongoing commercial or member relationship, without the need to check with the DNC Registry ('exempted messages').

6.8 Exempted messages must include information on how individuals can opt out of such messages using the same medium by which the message is sent. Upon receiving an individual's opt-out request, an organisation may no longer rely on the exemption and must stop sending such messages to that individual 30 days after the opt-out.

6.9 An "ongoing relationship" under the Exemption Order means a relationship which is on an ongoing basis, between a sender and a subscriber or user of a Singapore telephone number, arising from the carrying on or conducting of a business or activity (commercial or otherwise) by the sender. Factors in determining whether there is an ongoing relationship between a clinic and a patient could include:

a) The frequency of visits the patient makes to the clinic; and

b) The patient has agreed to a course of treatment that requires several separate visits to the clinic.

6.10 It should be noted that once-off transactions are insufficient to establish an ongoing relationship. The Advisory Guidelines on the Do Not Call Provisions provide further elaboration.

6.11	**Example: Messages that may fall within the Exemption Order** Clinic ABC regularly calls or sends text messages to its patients with chronic conditions at their Singapore telephone numbers to inform them about new drugs or medical procedures which the doctor considers could be effective treatment for their condition. Whether Clinic ABC has to first check the Do Not Call Registers to ensure that the Singapore telephone numbers are not listed would depend largely on whether the new drug or procedure relates to a medical condition for which Clinic ABC is providing ongoing treatment to the relevant recipients. *Example 1* John is undergoing treatment on an ongoing basis at Clinic ABC for his chronic asthma. Clinic ABC sends a text message to John to inform him about a new drug which could be effective treatment for his asthma. In this scenario, Clinic ABC's message could be considered an exempted message under the Exemption Order. *Example 2* Clinic ABC calls Sarah to inform her about a new drug which could be an effective treatment for asthma. Sarah has never sought treatment at Clinic ABC for asthma or asthma-related conditions, and does not have an ongoing relationship with Clinic ABC. In this scenario, Clinic ABC would not be able to avail itself of the Exemption Order and will need to check the Do Not Call Register before calling or sending a text message to Sarah, unless Clinic ABC had obtained clear and unambiguous consent in written or other accessible form from Sarah.

END OF DOCUMENT