PERSONAL DATA
PROTECTION COMMISSION
SINGAPORE

ADVISORY GUIDELINES FOR THE HEALTHCARE SECTOR

Issued 11 September 2014
Revised 20 September 2023

Supported by:

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

In support of:

SG:DIGITAL

TABLE OF CONTENTS

PART I: INTRODUCTION

1 Introduction

1.1 These Guidelines should be read in conjunction with the document titled "Introduction to the Guidelines", 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").

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 his personal data[1] and obtain his consent, unless any relevant exception to consent[2] applies. Moreover, organisations shall only collect, use and disclose personal data that are relevant for the purposes, and for purposes that a reasonable person would consider appropriate in the circumstances.

2.2 The following will highlight how consent may apply in common healthcare scenarios, how deemed consent applies as well as the exceptions to consent.

Deemed consent

2.3 *Deemed consent by conduct:* In situations where an individual (without actually giving consent) voluntarily provides his personal data to an organisation for an appropriate purpose, and it is reasonable that he would voluntarily provide the data, the individual's consent to the collection, use or disclosure of personal data is deemed to have been given by the individual's act of providing his personal data.

2.4 *Deemed consent by contractual necessity:* Pursuant to Section 15(3), if an individual gives, or is deemed to have given, consent to the collection, use or disclosure of his personal data to one organisation ("A") for the purpose of a contractual transaction, the consent may cover sharing of his personal data by A with other organisations (and onward sharing by downstream organisations, as the case may be) so long as it

[1] 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.

[2] Please refer to the First (collection, use and disclosure of personal data without consent) and Second (additional bases for collection, use and disclosure of personal data without consent) Schedules under the PDPA for any exceptions which may apply.

is reasonably necessary for A to provide the personal data to the other organisations (likewise, for onward sharing by downstream organisations) to perform or conclude A's contractual obligations.

2.5 *Deemed consent by notification:* Section 15A provides that if an individual does not take any action to opt out of the collection, use or disclosure of his personal data for a purpose that he has been notified of, the individual is deemed to consent to the collection, use or disclosure of personal data by the organisation even for secondary use purposes that are different from the primary purposes for which it had originally collected the personal data for[3]. Nonetheless, the individual must have been notified that their personal data would be used for such secondary use purposes. The organisation must meet stipulated conditions by conducting an assessment to identify any adverse impact on the individuals arising from the proposed collection, use or disclosure of his personal data, and implement mitigating measures in relation to the adverse impacts identified. Please refer to the Advisory Guidelines on Key Concepts in the PDPA (Chapter 12) for more information on the stipulated conditions.

Withdrawal of consent

2.6 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. Please refer to the Advisory Guidelines on Key Concepts in the PDPA (Chapter 12) for the requirements that must be complied with by either the individual or the organisation in relation to the withdrawal of consent. However, the organisation can continue to use and disclose personal data in their possession if allowed under other legal bases.

Exceptions to the Consent Obligation

2.7 Section 17 of the PDPA permits the collection, use and disclosure of personal data without consent (and, in the case of collection, from a source other than the individual) and enumerates the permitted purposes in the First and Second Schedules to the PDPA. These exceptions to the Consent Obligation do not affect rights or obligations arising under any other law. Hence, even if an exception applies under the PDPA, organisations are required to comply with their other legal obligations, for example, to protect confidential information or other contractual obligations.

[3] Primary purposes are the purposes for which the personal data was originally collected for. Secondary purposes are any purposes which the personal data is further used for after collection.

Legitimate interests exception

2.8 The term "legitimate interests" refers to any lawful interests of an organisation or other person (including other organisations). Organisations may collect, use and disclose personal data without consent where the identified legitimate interests outweigh any adverse effect on the individual. The "legitimate interests" exception encompasses either of the following:

a) The general "legitimate interests" exception (under paragraph 1 of Part 3 of the PDPA First Schedule) is a broad exception for any purposes that meet the definition of "legitimate interest". Organisations relying on this exception must assess and act upon any adverse effects on the individuals (i.e., whether to eliminate, reduce likelihood of or mitigate the adverse effects); or

b) The specific "legitimate interests" exception is confined to purposes prescribed within paragraphs 2 to 10 of Part 3 of the PDPA First Schedule such as for evaluative purposes, for any investigation or proceedings, or for recovery or payment of debt owed etc.

2.9 The "legitimate interests" exception allows the collection, use or disclosure of personal data without consent for a wide range of circumstances and purposes. Organisations relying on this exception would need to comply with additional safeguards to ensure the interests of individuals are protected and can refer to paragraphs 12.56 to 12.70 of the Advisory Guidelines on Key Concepts in the PDPA for more information. Organisations cannot rely on the legitimate interests exception to send direct marketing messages.

Business improvement exception

2.10 Part 5 of the First Schedule and Division 2 under Part 2 of the Second Schedule ("business improvement exception") enable organisations to use, without consent, **personal data that they had collected** in accordance with the Data Protection Provisions, so long as the use of the personal data falls within the scope of any of the following purposes:

a) Improving, enhancing or developing new goods or services;

b) Improving, enhancing or developing new methods or processes for business operations in relation to the organisations' goods and services;

c) Learning or understanding behaviour and preferences of individuals (including groups of individuals segmented by profile); or

d) Identifying goods or services that may be suitable for individuals (including groups of individuals segmented by profile) or personalising or customising any such goods or services for individuals.

2.11 To rely on the business improvement exception, organisations will need to ensure the following:

a) The business improvement purpose cannot reasonably be achieved without using the personal data in an individually identifiable form; and

b) The organisation's use of personal data for the business improvement purpose is one that a reasonable person would consider appropriate in the circumstances.

2.12 The business improvement exception also applies to the sharing of personal data (i.e., collection and disclosure) between entities belonging to a group of companies, without consent, for the following business improvement purposes:

a) Improving, enhancing or developing new goods or services;

b) Improving, enhancing or developing new methods or processes for business operations in relation to the organisations' goods and services;

c) Learning or understanding behaviour and preferences of **existing or prospective customers**[4] (including groups of individuals segmented by profile); or

d) Identifying goods or services that may be suitable for **existing or prospective customers** (including groups of individuals segmented by profile) or personalising or customising any such goods or services for individuals.

2.13 Organisations relying on this exception to share personal data within a group of entities need to ensure several conditions are fulfilled first. Organisations cannot rely on the business improvement exception to send direct marketing messages. For more information, please refer to paragraphs 12.71 to 12.77 of the Advisory Guidelines on Key Concepts in the PDPA.

[4] Existing customers refer to individuals who have a history of purchasing or hiring any goods or using any services provided by the organisation. Prospective customers generally refer to an individual who informs or has informed the organisation of his interest in its goods or services, which includes subscription to a mailing list, or an individual who is conducting negotiations to purchase or hire or use any goods or services provided by the organisation.

Research exception

2.14 The business improvement exception is intended to enable organisations to use personal data to improve their products, services, business operations and customer experience. On the other hand, the research exception enables organisations to conduct broader research and development that may not have any immediate application to their products, services, business operations or market. Commercial laboratories or institutes of higher learning that carry out research for the development of health products or medicine, and organisations that carry out market research are examples of organisations that can rely on the research exception. The research exception (Division 3 under Part 2 of the PDPA Second Schedule) provides that organisations may **use** personal data for a research purpose without consent, including historical and statistical research, subject to the following conditions:

a) The research purpose cannot reasonably be accomplished unless the personal data is provided in an individually identifiable form;

b) There is a clear public benefit to using the personal data for the research purpose;

c) The results of the research will not be used to make any decision that affects the individual; and

d) In the event the results of the research are published, the organisation must publish the results in the form that does not identify the individual[5].

2.15 Organisations may **disclose** personal data for a research purpose without consent, including historical and statistical research, by assessing the same set of conditions applicable to the research exception relating to use of personal data with an **additional condition:**

a) It is impracticable for the organisation to seek the consent of the individual for the disclosure.

2.16 When assessing whether it would be "impracticable" for the organisation to seek consent of the individual, the specific facts of the case have to be considered. For more information on the research exception, please refer to paragraphs 12.80 to 12.83 of the Advisory Guidelines on Key Concepts in the PDPA.

[5] Please refer to Chapter 3 on Anonymisation in the Advisory Guidelines on the PDPA for Selected Topics for more information.

2.17 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. Where appropriate, brief references may be made to other obligations, but it is not the intent to apply every obligation in the PDPA within each example.

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

John visits Hospital ABC for the first time for a medical examination. 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 Hospital ABC for the purpose of his visit, including any medical care 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 Hospital ABC; and
- the convening of a case conference with other doctors within Hospital ABC solely for the purpose of discussing treatment options for John.

There is likely to be deemed consent by conduct as the purposes for the collection, use and disclosure of John's personal data are objectively obvious and reasonably appropriate from the surrounding circumstances. As long as John actively provides his personal data to Hospital ABC or allows his personal data to be collected by Hospital ABC, deemed consent by conduct applies.

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

Deemed consent by conduct does not cover purposes outside those for which the personal data was provided. Generally, if Hospital ABC intends to use or disclose such personal data for purposes that are not related to provision of medical care, it

	is less likely to be covered by deemed consent by conduct and in such instances Hospital ABC should notify John of such purposes and obtain his consent. However, Hospital ABC may rely on deemed consent by notification to use or disclose existing data for secondary purposes that are different from the primary purposes for which it had been originally collected for, by conducting an assessment first to ensure several conditions are met and taking reasonable steps to ensure that John is notified of Hospital ABC's intention to collect, use or disclose his personal data and the purpose(s) of such collection, use or disclosure[6]. Deemed consent by notification cannot be relied on if John has opted out of the collection, use or disclosure of his personal data. For example, Hospital ABC may wish to use John's personal data for the marketing of health products that are unrelated to John's condition to John. 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 Hospital ABC or the provision of medical care related to his visit. Hospital ABC is unable to rely on deemed consent by notification where consent previously obtained from John is used for the secondary purpose of marketing health products by direct marketing messages that are unrelated to his condition. Therefore, Hospital ABC should notify John of such purposes and actively obtain his express 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, Hospital 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, Hospital ABC should not collect more personal data than is required for its business or legal purposes. It is also good practice for Hospital ABC to indicate which fields in the form that collect personal data are compulsory and which are optional. *How the Retention Limitation Obligation applies* Hospital 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, Hospital ABC may retain John's personal data in accordance with Regulation 12 of the Private Hospitals and Medical

[6] Please refer to Section 15A of the PDPA for details on assessment to be conducted for reliance on deemed consent by notification.

	Clinics ("PHMC") Regulations, the National Guidelines for Retention Periods of Medical Records under the PHMC Act, Regulation 37 of the Healthcare Services (General) Regulations and the Licence Conditions on the retention periods of patient health records under Healthcare Services Act (HCSA) (which, in brief, provides that licensed healthcare institutions must maintain medical records for such periods as may be required).
2.19	**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 Hospital 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 Hospital 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 Hospital 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 Hospital 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 Hospital ABC. An 'employee' under the PDPA includes a volunteer working under an unpaid volunteer work relationship.
2.20	**Example: Disclosing personal data in referral cases** During separate consultations with the following patients, Doctor Lee 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 Doctor Lee proceeds to make the necessary arrangements, for example, by contacting another doctor directly[7]. Since each patient agreed to the recommendation by the primary doctor, the patient would have consented to the doctor disclosing his personal data as required for the referral when contacting the proposed healthcare service provider directly. In cases where Doctor Lee 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, Doctor Lee could consider documenting the verbal consent given, such as by making a note in the patient's file. Having written evidence supporting verbal consent would be useful in the event of a dispute. Before Doctor Lee 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, and in compliance with any prevailing healthcare requirements and licensing conditions such as the PHMC Act and HCSA. For the avoidance of doubt, Doctor Lee 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.
2.21	**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 providing 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

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

	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 8(a) of Part 3 of the First Schedule to the PDPA[8], 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 solely for purposes consistent with the purpose of the collection, it may do so pursuant to paragraph 8(b) of Part 3 of the First Schedule to the PDPA[9]. 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. <u>If Aunt Kim cannot be identified</u> 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) makes an assessment that it 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. The onus is on the organisation to make the assessment and determine whether the PDPA is applicable to the data collected. For more information on the assessment that the organisation can make to determine if Aunt Kim can be identified from the data, please refer to paragraphs 5.4 to 5.6 of the Advisory Guidelines on Key Concepts in the PDPA.
2.22	**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:

[8] Under paragraph 8(a) of Part 3 of First Schedule to the PDPA, 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.

[9] Paragraph 8(b) of Part 3 of First Schedule to the PDPA allows organisations to collect, use or disclose personal data without consent for the purpose indicated in paragraph 8(a) of Part 3 of First Schedule to the PDPA. Please refer to the PDPA for more information.

	a) review of internal processes for quality assurance and other activities that are integral to the proper functioning of overall business operations; 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 obtains consent from John. In relation to the specific purposes above: a) <u>For internal quality assurance and other activities that are integral to the proper functioning of overall business operations</u>: 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[10]; and b) <u>For formulation of teaching material</u>: Health Organisation ABC should typically notify John of such purposes and obtain consent if the data cannot be anonymised. 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[11].) 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

[10] 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.

[11] 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.

	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 collected, used or disclosed for these purposes as a condition of providing him the medical care service (section 14(2)(a) of the PDPA). Even though the healthcare institution may be required by contractual obligation[12] to teach students or trainees and to formulate teaching materials, this contractual obligation cannot be a requirement for the provision of medical care to John. <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[13]. 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).
2.23	**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.

[12] Public healthcare institutions are subsidised by the government and the teaching of medical students is a charter of the public healthcare institutions.

[13] 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.

	This is pursuant to the vital interests exception under paragraph 2 of Part 1 of the First Schedule to the PDPA[14]. The hospital should also notify John's father, as soon as is practicable, of the collection, use or disclosure and the purpose for the collection, use or disclosure of his personal data.
2.24	**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 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 its 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.
2.25	**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

[14] Under paragraph 2 of Part 1 of the First Schedule to the PDPA, 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.

	engaged in by his employer for purposes of the PDPA[15]. Hence, Clinic ABC will have 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. However, Doctor Hussein will be held accountable if he egregiously mishandles the personal data in the possession of or under the control of Clinic ABC[16] or if he was not acting in the course of his employment when collecting, using or disclosing personal data. 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 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.
2.26	**Example: Acquisition of medical practice by another organisation**

[15] Section 53 of the PDPA provides that:

(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.

[16] Part 9B of the PDPA provides that individuals are held accountable for egregious mishandling of personal data in the possession of or under the control of an organisation (including a public agency). The offences are for knowing or reckless unauthorised: (1) disclosure of personal data, (2) use of personal data for a gain for the individual or another person, or to cause harm or a loss to another person, and (3) re-identification of anonymised information.

	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 of Part 4 of the First Schedule to the PDPA relating to business asset transactions could apply, subject to the conditions stated. Doctor Hussein is allowed to collect, use or disclose 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.
2.27	**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. The researcher's institutional review board (IRB) has also determined that this research is not regulated under the Human Biomedical Research Act (HBRA). 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, the results of the research will not be used to make specific decisions affecting the individuals and the benefits to be derived from the research are clearly in the public interest. In this case, Health Organisation ABC is able to use personal data about these individuals without consent, pursuant to the research exception in Division 3 under Part 2 of the Second Schedule to the PDPA. Health Organisation ABC also wishes to publish the results of its research in its website and newsletter. The results must be represented in a form that does not identify the past patients.

	Health Organisation ABC may also wish take into account the opinion of its Institutional Review Board ("IRB"), or equivalent body, which provides ethics approval for research projects.

3 The Access and Correction Obligations

3.1 The Access and Correction Obligations (PDPA sections 21, 22 and 22A) state that an organisation must, upon request, (i) provide an individual with his or her personal data in the possession or under the control of the organisation and information about the ways in which the personal data may have been used or disclosed during the past year; and (ii) correct an error or omission in an individual's personal data that is in the possession or under the control of the organisation. For more information on the Access and Correction Obligations, do refer to Chapter 15 of the Advisory Guidelines on Key Concepts in the PDPA.

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

3.3 **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 2022.

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. *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. The goal is to provide John with an account of his personal data that is contained in the document and how it has been used or disclosed. Where this goal is more easily achieved through a redacted document provided to John, redaction can be considered. In certain circumstances, it may be impracticable to redact the handwritten notes and still provide a redacted document that is intelligible. The clinic has to take into consideration what is reasonable in the circumstances and whether the mode of providing access enables John to understand how his personal data had been used or disclosed. <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 2021 to 5th December 2022, 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.

	<u>Rejecting an access request</u> If the clinic rejects John's access request based on an exception from the Access Obligation under the Fifth Schedule to the PDPA, the clinic shall provide a reply to John and inform him of the relevant reason(s) for refusing his request. In this case, the clinic is still required to preserve a complete and accurate copy of John's personal data for a period of at least 30 calendar days after rejecting the access request, as John may seek a review of the clinic's decision. 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.
3.4	**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 Accuracy, Protection, Retention Limitation, Transfer Limitation, Data Breach Notification and Accountability 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.

The Accuracy Obligation

4.2 Pursuant to the Accuracy Obligation (PDPA section 23), an organisation must make a reasonable effort to ensure that personal data collected by or on behalf of the organisation is accurate and complete if the personal data is likely to be used by the organisation to make a decision that affects the individual concerned or disclosed by the organisation to another organisation. For more information on the Accuracy Obligation, do refer to Chapter 16 of the Advisory Guidelines on Key Concepts in the PDPA.

The Protection Obligation

4.3 According to the Protection Obligation (PDPA section 24), an organisation must protect personal data in its possession or under its control by making reasonable security arrangements to prevent (i) unauthorised access, collection, use, disclosure, copying, modification or disposal, or similar risks; and (ii) the loss of any storage medium or device on which personal data is stored. For more information on the Protection Obligation, do refer to Chapter 17 of the Advisory Guidelines on Key Concepts in the PDPA.

The Retention Limitation Obligation

4.4 The Retention Limitation Obligation (PDPA section 25) states that an organisation must cease to retain 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 (i) the purpose for which the personal data was collected is no longer being served by retention of the personal data; and (ii) retention is no longer necessary for legal or business purposes.

4.5 The PDPA does not prescribe a specific retention period for personal data. However, healthcare institutions should review the personal data they hold on a regular basis to determine if that personal data is still needed. The retention period for personal data under the PDPA can depend on whether the personal data is required for research or archival purposes that benefit the wider public or a segment of the public. 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, Regulation 37(1) of the Healthcare Services (General) Regulations, and the MOH's *2022 Revised Guidelines for the Retention Periods of Medical Records*. For more information on the Retention Limitation Obligation, do refer to Chapter 18 of the Advisory Guidelines on Key Concepts in the PDPA.

The Transfer Limitation Obligation

4.6 The Transfer Limitation Obligation (PDPA section 26) states that an organisation must not transfer personal data to a country or territory outside Singapore except in accordance with the requirements prescribed under the PDPA. For more information on the Transfer Limitation Obligation, do refer to Chapter 19 of the Advisory Guidelines on Key Concepts in the PDPA.

The Data Breach Notification Obligation

4.7 The Data Breach Notification Obligation (PDPA sections 26A to 26E) states that an organisation must assess whether a data breach is notifiable and notify the affected individuals and/or the Commission where it is assessed to be notifiable. For more information on the Data Breach Notification Obligation, do refer to Chapter 20 of the Advisory Guidelines on Key Concepts in the PDPA.

The Accountability Obligation

4.8 The Accountability Obligation (PDPA sections 11 and 12) states that an organisation must implement the necessary policies and procedures in order to meet its obligations under the PDPA and shall make information about its policies and procedures publicly available. For more information on the Accountability Obligation, do refer to Chapter 21 of the Advisory Guidelines on Key Concepts in the PDPA.

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 3 to 6 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 3 to 6 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 3 to 6 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, HCSA, 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 4 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 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[17] 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 to the PDPA, 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 a 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;

d) any message that is sent while the sender is in an ongoing relationship with the recipient of the message; and the sole purpose of which relates to the subject matter of the ongoing relationship; or

e) 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.

[17] 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 (DNC) Registry, unless 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.

6.6 The PDPA lists obligations for third-party checkers[18] who check the DNC Registry for an organisation and provide to the organisation information on whether the Singapore telephone number is listed in the relevant DNC Register. The checker must make sure that information provided to the organisation is accurate and up-to-date in accordance with the provisions relating to the DNC Registry[19], and to provide to the organisation the date of retrieval of this information and its validity period.

[18] Please refer to section 43A of the PDPA for definition of a third-party checker and the full set of obligations for checkers.

[19] Including Part 5A of the Personal Data Protection (Do Not Call Registry) Regulations 2013.

6.7	**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. If Clinic ABC had engaged by contract a third-party checker that helps to check the DNC Registry, the third-party checker is responsible for checking that the information on whether Peter's number is listed is accurate and up-to-date. *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. In addition, the sole purpose of Dental Clinic DEF sending the reminder text messages is to facilitate the transaction that Jason has previously agreed to. Therefore, Dental Clinic DEF may send such messages to Jason without checking the Do Not Call Registry.

6.8	**Example: Messages where the sender is in an ongoing relationship with the recipient** 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 can be excluded from the meaning of "specified message" in the Eighth Schedule to the PDPA and is not subject to the DNC provisions. *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 will not be able to rely on the exclusions listed under the Eighth Schedule to the PDPA 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. For clarity, even if Sarah was undergoing treatment at Clinic ABC for another medical condition (e.g. migraines), Clinic ABC must comply with the DNC provisions when it sends a marketing message to Sarah about an unrelated condition (e.g. asthma).

Dictionary Attacks and Address-Harvesting Software

6.9 Section 48B of the PDPA provides that organisations must not send, cause to be sent, or authorise the sending of messages to recipient telephone numbers that are obtained by dictionary attack or address-harvesting. Dictionary attack is the method by which the telephone number is obtained using automated means that generate possible telephone numbers by combining numbers into numerous permutations, whereas address-harvesting is a software specifically designed or marketed for use for searching the Internet for telephone numbers and the telephone numbers are collected, compiled, captured or otherwise harvested.

END OF DOCUMENT