

Personal Data Protection Policy of ISEC Healthcare Ltd and its Affiliated Companies

30 September 2022



Document Reviewers/Approvals

Version	Reviewed & Approved By	Date
1	CFO	1 July 2015
2	CFO	31 May 2017
3	CEO	30 September 2022



Personal Data Protection Policy of ISEC Healthcare Ltd and its Affiliated Companies **Version 3.0**

REVISION HISTORY

Date	Version	Change Description	Actors
1 July 2015	1.0	First version	Preparer: RHT Law Taylor Wessing LLP Reviewer/Approver: Macy Thong, CFO
31 May 2017	2.0	Updated policy	Preparer: Elyse Low, Finance Manager Reviewer/Approver: Macy Thong, CFO
30 September 2022	3.0	Updated policy	Preparer: Maggie Ge, Director of Operations Reviewer/Approver: Dr Wong Jun Shyan, CEO



Table of Contents

INTRODUCTION	4
OVERVIEW OF THE PDPA	4
PURPOSE	4
BUSINESS CONTACT INFORMATION	5
OBLIGATIONS UNDER THE PDPA	5
KEY OBLIGATIONS OF DATA PROTECTION	5
CONSENT FOR COLLECTION, USE OR DISCLOSURE OF PERSONAL DATA.....	6
NOTIFICATION OF PURPOSE	6
USE OF PERSONAL DATA COLLECTED PRIOR TO 2 JULY 2014.....	7
DISCLOSURE OF PERSONAL DATA.....	7
ACCESS TO PERSONAL DATA.....	8
ACCURACY AND CORRECTION OF PERSONAL DATA.....	8
TRANSFER OF PERSONAL DATA OUTSIDE SINGAPORE	9
SECURITY.....	9
MANAGING CCTV AND OTHER FORMS OF AUDIO AND VISUAL RECORDING	10
MARKETING MESSAGES.....	10
RETENTION AND DESTRUCTION	10
COMPLAINTS.....	11
HANDLING OF PERSONAL DATA OF ISEC STAFF.....	11
CONSEQUENCES OF NON-COMPLIANCE.....	11
APPOINTMENT AND DUTIES OF THE DATA PROTECTION OFFICER	12
RESPONSIBILITIES OF THE DPO	12
ANNEX A.....	13
ANNEX B.....	19
ANNEX C.....	22
ANNEX D.....	23
ANNEX E	29
ANNEX F	36
ANNEX G.....	37



Personal Data Protection Policy of ISEC Healthcare Ltd and its Affiliated Companies Version 3.0

1. INTRODUCTION

- 1.1 ISEC Healthcare Ltd and its related and affiliated companies (collectively “**ISEC**”) respect the right of Individuals to protect their personal data. ISEC is committed to protecting the privacy of every Individual’s personal data in accordance with its obligations under the Personal Data Protection Act 2012 (“**PDPA**”).
- 1.2 To comply with our obligations under the PDPA, we have produced this Personal Data Protection Policy (“**Policy**”). This Policy sets out what we must do when any personal data of an Individual is collected, used or disclosed and it also seeks to provide general guidance as to how to collect, handle, store or transmit personal data that we may receive in the course of administering the affairs of ISEC.
- 1.3 This Policy applies to all personnel of ISEC, which includes all Doctors, Clinical Staff and Administrative Staff, whether employed on a full-time or part-time basis. All personnel of ISEC must familiarize themselves and comply with the obligations, policies and practices set out in this Policy.
- 1.4 Compliance with the PDPA is important, because a failure to observe the obligations under the PDPA could potentially expose ISEC, Doctors, Clinical Staff and Administrative Staff to complaints, criminal charges and/or bad publicity. Any failure by personnel of ISEC to comply with the PDPA may lead to disciplinary action for serious or repeated breaches and/or a report being made to the Police, the Personal Data Protection Commission and any other relevant government authority.

OVERVIEW OF THE PDPA

2. The PDPA came into effect on 2 January 2013 with the main personal data protection provisions coming into force on 2 July 2014.
3. Purpose
 - 3.1 The PDPA is concerned with the protection of “Personal Data”, which is defined as any data, whether true or not, about an Individual who can be identified from that data or from that data and other information that an organisation has access to. The PDPA seeks to balance the rights of an Individual to protect his/her personal data and the need of organisations to collect, use and disclose personal data for purposes that a reasonable person would consider appropriate in the circumstances.

4. Business Contact Information

- 4.1 The PDPA does not apply to “Business Contact Information”, such as an Individual’s name, position or title, business telephone number and fax number, business address, business email address and any other similar information about the Individual, which was given for commercial purposes or for a non-personal purpose.
- 4.2 However, if a person gives his Business Contact Information to ISEC to receive goods or services from ISEC for his personal purposes (in other words, he/she wants ISEC to contact him/her at his/her office rather than his/her home), then the business contract information of that person will be personal data for the purposes of the PDPA.

OBLIGATIONS UNDER THE PDPA

5. Key Obligations of Data Protection

- 5.1 The PDPA sets forth 9 obligations governing the collection, use, disclosure and care of personal data that must be observed by all organizations that handle personal data. The 9 obligations are:
- (a) Consent Obligation (sections 13-16 PDPA);
 - (b) Purpose Limitation Obligation (section 18 PDPA);
 - (c) Notification of Purpose Obligation (section 20 PDPA);
 - (d) Obligation to grant Access to Personal Data (section 21 PDPA);
 - (e) Correction of Personal Data (section 22 PDPA);
 - (f) Accuracy of Personal Data (section 23 PDPA);
 - (g) Obligation to Protect (Keep Secure) Personal Data (section 24 PDPA);
 - (h) Retention Obligation (section 25 PDPA); and
 - (i) Transfer of Personal Data Outside of Singapore Obligation (section 26 PDPA).

6. Consent for Collection, Use or Disclosure of Personal Data

- 6.1 We will obtain the consent of our patients and employees (collectively “**Individuals**”) before we collect use, or disclose their personal data. In obtaining consent, we will use reasonable efforts to ensure that the Individual is advised of the identified purposes for which his/her personal data is being collected, used or disclosed. Purposes will be stated in a manner that can be reasonably understood by the Individual.



Personal Data Protection Policy of ISEC Healthcare Ltd and its Affiliated Companies ***Version 3.0***

- 6.2 We will seek consent to use and disclose personal data at the same time as we collect the personal data. If we intend to use or disclose the personal data for a new purpose that was not previously identified, we will seek consent to use and disclose the personal data before it is used or disclosed for the new purpose.
- 6.3 We will collect personal data directly from Individuals, but we may also collect personal data from other sources including relatives or personal references or other third parties provided they have the right to disclose such personal data.
- 6.4 We will limit the type of personal data collected to that which is necessary for the purposes that we have identified.
- 6.5 An Individual may withdraw consent at any time, subject to legal or contractual restrictions and reasonable notice. An Individual may contact us for more information regarding the implications of withdrawing consent.
- 6.6 In certain circumstances, personal data can be collected, used or disclosed without the consent of the Individual. For example:
- (a) the collection, use or disclosure is necessary for any purpose that is clearly in the interest of the Individual, if consent for its collection, use or disclosure cannot be obtained in a timely way or the Individual would not reasonably be expected to withhold consent, such as when the Individual is seriously ill or mentally incapacitated;
 - (b) the collection, use or disclosure is necessary to respond to an emergency that threatens the life, health or safety of the Individual or another Individual;
 - (c) the collection, use or disclosure is necessary for any investigation or proceedings, if it is reasonable to expect that seeking the consent of the Individual would compromise the availability or the accuracy of the personal data;
 - (d) the collection, use or disclosure is necessary for evaluative purposes;
 - (e) the personal data was provided to the Company by another Individual to enable the Company to provide a service for the personal or domestic purposes of that other Individual.

7. Notification of Purpose



Personal Data Protection Policy of ISEC Healthcare Ltd and its Affiliated Companies Version 3.0

- 7.1 We will identify the purposes for which we collect, use or disclose personal data on or before we collect, use or disclose the personal data of Individuals. Upon receipt of the personal data, we will use or disclose the personal data only for the identified purpose and for purposes that a reasonable person would consider appropriate in the circumstances.
- 7.2 We generally collect, use and disclose personal data for the following purposes:
- (a) To manage the administration, finances, and operations of ISEC;
 - (b) To provide our services to Individuals;
 - (c) To establish and maintain responsible relationships with Individuals; and
 - (d) To meet our legal and regulatory obligations.
- 7.3 As a general rule, ISEC must obtain consent from Individuals before collecting their personal data and, in obtaining consent, will notify the Individuals of the purpose for the collection and the intended use of their personal data. This includes all personal data collected for treatment or employment or any other related purpose. ISEC must ensure that all personal data collection efforts are accompanied with the appropriate notifications and personal data collection clauses. Sample personal data collection notifications, clauses and supplements for patients, job applicants and employees are set out at **Annexes B, C and D** respectively.
- 7.4 When personal data that has been collected is to be used or disclosed for a purpose not previously notified, the new purpose will be notified to Individuals prior to use. Unless the new purpose is permitted or required by law, consent will be required before the personal data will be used or disclosed for the new purpose.
8. Use of Personal Data Collected Prior to 2 July 2014
- 8.1 Personal data collected prior to 2 July 2014, when the main provisions of the PDPA on the protection of personal data came into force, can continue to be used or disclosed but only for the purpose that the personal data was originally collected, unless an Individual has withdrawn his/her consent for such continued use or disclosure of his/her personal data.
- 8.2 If there is a new purpose for the use or disclosure of existing personal data, a fresh consent has to be obtained from the Individuals for this new purpose.
9. Disclosure of Personal Data
- 9.1 Generally, only the Doctors, Clinical Staff and Administrative Staff with a need to know or whose duties or services reasonably require access to personal data are granted access to personal data about the Individuals through our Electronic Medical Records.

Personal Data Protection Policy of ISEC Healthcare Ltd and its Affiliated Companies ***Version 3.0***

- 9.2 Where we are required to disclose personal data to third parties (such as to other healthcare organisations), a note will be made against that Individual's personal data of the disclosure.
- 9.3 Where personal data must be disclosed to a third party (e.g. external vendor), ISEC must ensure that the contract with the third party contains an appropriate personal data protection clause. A sample personal data protection clause and supplement for use in connection with third party contracts are set out in **Annex E**.

10. **Access to Personal Data**

- 10.1 All requests for access to personal data must be directed to the Data Protection Officer and to management.
- 10.2 Upon receipt of a written request from an Individual and after verifying the Individual's identity, we will provide the Individual with a reasonable opportunity to review the personal data that we have about the Individual in our possession or under our control. Personal data will be provided within a reasonable time and at minimal cost to cover administrative expenses. If we are unable to respond within 30 days of receiving the written request, we will inform the Individual in writing of the time by which we will respond to his/her request.
- 10.3 Upon receipt of a request from an Individual, we will provide an account of the use and disclosure of the personal data of the Individual. In providing an account of disclosure, we will provide a list of the organisations to which we may have disclosed personal data about the Individual.
- 10.4 In certain situations we may not be able to provide access to all of the personal data we hold about an Individual; for instance:
- (a) If doing so would likely reveal personal data about another Individual or could reasonably be expected to threaten the life or security of another Individual;
 - (b) If doing so would reveal any confidential information;
 - (c) If the information is protected by legal privilege;
 - (d) If the information was generated in the course of a formal dispute resolution process; or
 - (e) If the information was collected in relation to the investigation of a contravention of a law or a breach of an agreement.
- 10.5 In such a case, we will provide the reasons for denying access to the personal data.

11. **Accuracy and Correction of Personal Data**



Personal Data Protection Policy of ISEC Healthcare Ltd and its Affiliated Companies ***Version 3.0***

- 11.1 We will endeavor to ensure that the personal data collected will be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used. Ensuring that the personal data that we possess is sufficiently accurate, complete and up-to-date will help minimize the possibility that inappropriate decisions are being made based on inaccurate or incomplete or outdated information.
- 11.2 We will promptly correct or complete any personal data found to be inaccurate or incomplete. Upon receipt of a request from an Individual to correct or update his/her personal data, we will promptly correct or update his/her personal data.
- 11.3 Where we are not able to confirm the accuracy or completeness of an Individual's personal data (such as those Individuals who have emigrated or who are no longer contactable) or where we are not able to make a requested correction (such as changing a diagnosis about a medical condition), a note will be made against that Individual's personal data of the corrections which were requested and/or the potential unresolved differences.
- 11.4 Where appropriate, we will inform third parties having access to the personal data in question of any amended personal data or the existence of any unresolved differences.
- 11.5 We will conduct an exercise periodically to update the personal data of the Individuals.

12. Transfer of Personal Data Outside of Singapore

- 12.1 We will protect personal data disclosed to third parties by contractual or other means stipulating the purposes for which it is to be used and the necessity to provide a comparable level of protection.
- 12.2 We will not transfer any personal data to any organisation located in a country or territory outside Singapore unless that other organisation is subject (whether by way of legislation or contractual arrangement) to obligations of protection of personal data that are comparable to those under the PDPA.
- 12.3 Where we are required to transfer personal data to third parties, a note will be made against that Individual's personal data of the transfer.

13. Security

- 13.1 We have the responsibility under the PDPA to make reasonable security arrangements to protect the personal data that we possess or control to prevent unauthorised access, collection, use, disclosure or similar risks.

Personal Data Protection Policy of ISEC Healthcare Ltd and its Affiliated Companies ***Version 3.0***

13.2 We will use appropriate security measures to protect personal data against such risks as loss or theft, unauthorised access, disclosure, copying, use, modification or destruction, regardless of the format in which the personal data is held.

13.3 Any suspected or actual breach of security pertaining to personal data in our possession or control must be reported to the head of department and the Data Protection Officer for investigation.

14. Managing CCTV and other forms of Audio and Visual Recording

14.1 All audio and visual recordings, including videos and photographs, are considered personal data under the PDPA. Therefore appropriate measures must be taken to obtain consent and notify Individuals of such recordings.

14.2 We operate close circuit television (CCTV) cameras in ISEC premises for security and operational purposes. ISEC will put up appropriate and visible signage at appropriate locations to notify the public that ISEC premises are monitored by CCTV. Except for security purposes, we will not use the CCTV cameras to identify an Individual personally.

14.3 We do not permit members of the public or patients to take photographs or film videos in ISEC's premises. Photographs and videos may be taken by our personnel during ISEC events and activities. As it is not practical to obtain the permission of each and every Individual attending the event or activity to have their photographs taken, ISEC should announce prior to or at the start of the event that photographs or videos may be taken during the event and if an Individual does not wish to have his/her photograph taken, he/she should notify ISEC or the photographers.

14.4 If an Individual makes the request after the photograph or video has been taken, ISEC should either delete the photographs or video frames where the Individual's image appear or pixelate the image of the Individual from the photographs or the video frames.

15. Marketing Messages

15.1 Starting from 2 January 2014, the Do Not Call Provisions of the PDPA imposes various restrictions and obligations on organisations who wish to send marketing messages to Singapore telephone numbers, including mobile, fixed-line, residential and business numbers.

15.2 Marketing messages generally refer to text messages, fax messages or voice calls which offer to supply, advertise or promote goods or services.

15.3 As a rule, ISEC does not send marketing messages to Singapore telephone numbers or to Individuals whose personal data is in our possession or control.

16. Retention and Destruction



Personal Data Protection Policy of ISEC Healthcare Ltd and its Affiliated Companies ***Version 3.0***

- 16.1 We will keep personal data only as long as it remains necessary or relevant for the identified purposes or as required by law.
- 16.2 Once the personal data in our possession or control is no longer necessary for administrative, business or legal purpose, we will destroy or erase the personal data or remove the means by which the personal data can be associated with particular Individuals (such as by way of anonymising the personal data).

17. Complaints

We will attend to and investigate any complaints concerning any possible breach of this Policy. If a complaint is found to be justified, we will take appropriate and prompt measures to resolve the complaint including, if necessary, amending our policies and procedures. The complainant will be informed of the outcome of the investigation regarding his/her complaint.

18. **Handling of Personal Data of ISEC Staff**

- 18.1 The personal data of Doctors, Clinical Staff and Administrative Staff, whether permanent or temporary, (collectively "**ISEC Staff**") will be used only for purposes connected with their employment with ISEC and for as long a period as is necessary following the termination of their employment.
- 18.2 We value the privacy of our ISEC Staff and shall process the personal data of our ISEC Staff in a fair and lawful manner. We will endeavour to comply with the obligations under the PDPA on the use of personal data in an employer-employee relationship.
- 18.3 From time to time, we may need to disclose some information held about ISEC Staff to government agencies, such as the Ministry of Manpower and the Central Provident Fund Board, and other relevant third parties, such as insurers, medical clinics and hospitals, solely for purposes connected with managing the employment of ISEC Staff and providing for his/her welfare during his/her employment with ISEC.

19. **Consequences of Non-Compliance**



Personal Data Protection Policy of ISEC Healthcare Ltd and its Affiliated Companies Version 3.0

- 19.1 Failure to comply with the provisions of the PDPA may expose ISEC to an investigation by the Personal Data Protection Commission (the “**PDPC**”) of the non-compliance.
- 19.2 If the PDPC is satisfied that ISEC is not complying with its obligations under the PDPA, the PDPC may give ISEC such directions as it thinks fit in the circumstances, which may include directions to:
- (a) stop collecting, using or disclosing personal data in contravention of the PDPA;
 - (b) destroy personal data collected in contravention of the PDPA;
 - (c) provide access to or correct the personal data in such manner and within such time as the PDPC may specify; or
 - (d) pay a financial penalty of up to S\$1 million.

20. Appointment and Duties of the Data Protection Officer

- 20.1 ISEC is required, as part of its compliance with the PDPA, to designate at least one person as its Data Protection Officer (“**DPO**”).
- 20.2 It should be noted that the designation of a DPO does not relieve ISEC of its legal obligations under the PDPA.

Responsibilities of the DPO

- 20.3 The DPO is responsible for ensuring that ISEC complies with the PDPA. The DPO must keep fully up to date with the requirements of the PDPA and ensure that all personnel who handle personal data are fully aware of these requirements.
- 20.4 Where appropriate, the DPO may delegate some of his responsibilities as DPO to other Individuals to ensure that ISEC complies with the PDPA.
- 20.5 In addition to ensuring that ISEC complies with the PDPA, the DPO is also responsible for dealing with queries and requests from Individuals in relation to ISEC’s data protection policies and practices.
- 20.6 The contact information of the DPO must be made available to the public. It may be in the form of ISEC office address or a general e-mail address.

ANNEX A

FREQUENTLY ASKED QUESTIONS

[The copyright in the following FAQ belongs to the Personal Data Protection Commission and is reproduced below for internal, non-commercial and informational purposes only. No part of the FAQ shall be displayed, distributed or otherwise used for any commercial purpose except with the prior written consent of the Personal Data Protection Commission.]

Collection, Use & Disclosure

1. How much personal data can an organisation collect, use or disclose?

Under the PDPA, an organisation may collect, use or disclose personal data only for reasonably appropriate purposes under the circumstances. Organisations should notify individuals of the purposes for the collection, use and disclosure of personal data, and seek individuals' consent for the collection, use and disclosure of the personal data unless an exception under the PDPA applies. These exceptions are set out in the Second, Third and Fourth Schedules of the PDPA respectively.

In this regard, organisations shall not, as a condition of supplying a product or service, require an individual to consent to the collection, use or disclosure of personal data beyond what is reasonable to provide the product or service. If the organisation wishes to collect any additional personal data, the organisation may provide the individual the option of whether to consent to this.

For example, an organisation selling a consumer product to individuals should not require them to reveal their annual household income as a condition of selling the product, although it may ask them to provide such personal data as an optional field.

2. What can an organisation do with respect to existing personal data collected before the effective date of the data protection rules on 2 July 2014?

Generally, organisations may continue to use the personal data collected prior to the effective date of the data protection rules, unless the individual withdraws consent (if consent had previously been given) or indicates that he does not consent to such use of the personal data.

Consent will need to be obtained if the existing data is to be used for a new purpose different from the purpose for which it was collected, or if the existing data is to be disclosed to another organisation or individual, unless any exception applies. These exceptions are set out in the Second, Third and Fourth Schedules of the PDPA respectively. This includes exceptions catering to certain emergency situations, investigations, publicly available data or where the personal data is used for evaluative purposes.

Personal Data Protection Policy of ISEC Healthcare Ltd and its Affiliated Companies* *Version 3.0

For example, if a company has been using its customer's personal data to provide after-sales customer support prior to the PDPA, it can continue to do so after the PDPA comes into effect, even if it did not obtain consent previously. However, if it now intends to use the same personal data for direct marketing where it had not collected the personal data for this purpose, consent will need to be obtained for such a purpose. If the organisation wishes to use the personal data for telemarketing, it will separately have to ensure compliance with the DNC provisions under the PDPA.

3. How can an organisation obtain an individual's consent for the collection, use or disclosure of his or her personal data?

Consent can be obtained in a number of different ways. As a best practice, an organisation should obtain consent that is in writing or recorded in a manner that is accessible for future reference, for example, if the organisation is required to prove that it had obtained consent.

An organisation may also obtain consent verbally although it may correspondingly be more difficult for an organisation to prove that it had obtained consent. For such situations, it would be prudent for the organisation to document the consent in some way.

4. Is the failure to opt out a form of consent?

Deeming that an individual has given his consent through inaction on his/her part will not be regarded as consent in all situations. Whether or not a failure to opt out can be regarded as consent will depend on the actual circumstances and facts of the case. Organisations are advised to obtain consent from an individual through a positive action of the individual to consent to the collection, use and disclosure of his personal data for the stated purposes.

5. Can an organisation selling databases containing personal data to other organisations continue to do so after the PDPA comes into effect?

An organisation may use personal data collected before 2 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.

If an organisation intends to disclose the personal data on or after the appointed day (other than disclosure that is necessarily part of the organisation's use of the personal data), the organisation must comply with the data protection provisions in relation to such disclosure. As the sale of databases containing personal data involves a disclosure of personal data, organisations must obtain valid consent from the relevant individuals before doing so.

6. Do organisations need to obtain consent from their employees before disclosing their personal data for the purpose of business merger or acquisition?

The PDPA provides for certain exceptions to the requirement to obtain consent. One of these exceptions allows organisations to collect, use or disclose personal data without consent for the purpose of “business asset transactions”, subject to certain conditions. “Business asset transaction” is defined in the PDPA and can apply to mergers and acquisitions.

For example, Organisation A is a prospective buyer of Organisation B. Organisation A can collect personal data without consent (and Organisation B can disclose without consent) about B’s employees, customers, directors or shareholders if it relates directly to the business with which the acquisition is concerned. The personal data must be necessary for Organisation A to determine whether to proceed with the acquisition, and organisations A and B must have entered into an agreement that requires A to use or disclose the personal data solely for purposes related to the acquisition.

For full details, please refer to the Second Schedule, paragraph 1(p) and 3 and Fourth Schedule, paragraph 1(p) and 3 of the PDPA.

7. Do prospective employers need to obtain consent from job applicants for the collection of their personal data from their past employers for evaluating the job applicant?

Organisations may collect, use and disclose personal data without consent where this is necessary for evaluative purposes. The term “evaluative purpose” is defined in section 2(1) of the PDPA and includes, amongst other things, the purpose of determining the suitability, eligibility or qualifications of an individual for employment, promotion in employment or continuance in employment.

Hence, the evaluative purpose exception allows employers to collect, use and disclose personal data without the consent of the individual concerned for various purposes that are common in the employment context, for example:

- a) Obtaining a reference from a prospective employee’s former employer where necessary to determine his suitability for employment; or
- b) Obtaining opinions about the employee where necessary to determine his eligibility for promotion.

In practice, an organisation that has been requested to disclose information about its past employee may not be able to evaluate whether it is necessary for evaluative purposes, and may therefore wish to obtain the consent of the individual.

8. Do organisations have to provide notifications when CCTVs are deployed? What should CCTV notices state?

Organisations must notify individuals of the purposes for which their personal data (including CCTV footage of them) is collected, used or disclosed and obtain their consent, unless any exception applies. For example, notification and consent is not required if the personal data is publicly available. The PDPA does not prescribe the content of notifications. Generally, organisations should indicate that CCTVs are operating in the premises, and the purpose of the CCTVs if such purpose may not be obvious to the individual.

Access & Correction

1. Must an organisation always provide access to an individual's personal data when a request is made?

An organisation is required to respond to an access request in respect of personal data in its possession as well as personal data that is under its control. However, organisations are prohibited from providing an individual access to his personal data if the provision of the data could reasonably be expected to:

- cause immediate or grave harm to the individual's safety or physical/mental health;
- threaten the safety or physical/mental health of another individual;
- reveal personal data about another individual;
- reveal the identity of another individual who has provided the personal data, and the individual has not consented to the disclosure of his or her identity; or
- be contrary to national interest.

In addition, there are cases where organisations may deny access requests. For example, organisations will not be required to provide access to personal data if it is subject to legal professional privilege, or if the disclosure of the information would reveal confidential commercial information that could harm the competitive position of the organisation. There are also exclusions for access and correction of personal data with respect to any examination conducted by an education institution, examination scripts and examination results prior to their release. Organisations may also refuse access to or refuse to correct opinion data kept solely for an evaluative purpose as defined in the PDPA. The specific exceptions may be found in section 21 and the Fifth Schedule of the PDPA.

2. What personal data must an organisation provide when an individual submits an access request?

Personal Data Protection Policy of ISEC Healthcare Ltd and its Affiliated Companies ***Version 3.0***

An organisation that receives an access request from an individual is required to provide the information requested by the individual. This may include:

- the individual's personal data (as specified in the request); and
- information about the ways the personal data has been or may have been used or disclosed by the organisation (as specified in the request).

3. Can an organisation charge a fee for access requests?

Organisations may charge an individual a reasonable fee for access to personal data about the individual. The purpose of the fee is to allow organisations to recover the incremental costs of responding to the access request, such as the cost of producing a physical copy of the personal data requested. To allow for greater flexibility, there is no prescribed amount of fees imposed on organisations.

As organisations are required to make the necessary arrangements to provide for standard types of access requests, the costs incurred in capital purchases (for example, purchasing new equipment to provide access to the requested personal data) should not be transferred to individuals. If the organisation chooses to charge a fee for an access request, the fee should accurately reflect the time and effort required to respond to the request.

4. Must an organisation provide correction to an individual's personal data when a request is made?

Upon request, an organisation is generally required to correct an error or omission and send the corrected personal data to every other organisation to which the personal data was disclosed to within a year before the correction, unless the other organisation does not need the corrected personal data for any legal or business purpose.

For example, the organisation may have disclosed a customer's name and address to a delivery company it engaged on a once-off basis to deliver a product that the customer purchased. Since the delivery has been completed, the organisation will not be required to send the corrected personal data to the delivery company.

An organisation need not make a correction where it is satisfied on reasonable grounds that a correction should not be made. In this case, the organisation shall annotate the personal data in its possession or under its control with the correction that is requested but not made. An organisation is also not required to alter an opinion, including a professional or expert opinion. Exceptions from correction requirement may be found in the Sixth Schedule of the PDPA.

5. Can an organisation charge a fee for correction requests?



Personal Data Protection Policy of ISEC Healthcare Ltd and its Affiliated Companies* *Version 3.0

Organisations are not entitled to impose a fee for the correction of personal data required under the PDPA.

Care of Personal Data

1. How long can an organisation retain its customers' personal data?

The PDPA does not prescribe the retention period of personal data. However, an organisation should 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 of collection is no longer served by the retention; and retention is no longer necessary for business or legal purposes.

Organisations are not required to delete or destroy a customer's personal data upon the customer's request, and may retain it as long as there is a business or legal reason to do so.

2. What are the rules on transferring personal data out of Singapore?

The PDPA requires that measures are taken by the organisation transferring the personal data overseas to ensure a comparable standard of protection of the personal data overseas. These measures include the use of contractual agreements among the organisations involved in the transfer conditions, for example, by ensuring that the recipient overseas is bound by legally binding obligations to provide a comparable standard of protection. These measures are set out in the Personal Data Protection Regulations 2014.



ANNEX B

**SAMPLE PERSONAL DATA COLLECTION NOTIFICATION AND CLAUSE
FOR PATIENTS / CUSTOMERS**

Introduction

This Annex B sets out in Section 1, a bilingual English and Chinese notice on collection of personal data which is meant for display by ISEC at clinic reception desks, and in Section 2, a data protection collection clause for use by ISEC in its consent forms and contracts for patients / customers.

Section 1 - Notice for Display at Clinic Counters

[The following notice to be displayed at the clinic reception desk.]

Notice

通知

The data protection provisions of the Personal Data Protection Act 2012, which govern the collection, use and disclosure of personal data, came into effect on 2 July 2014. **International Specialist Eye Centre Singapore Pte. Ltd. ("ISEC Singapore")** is committed to handling all personal data which we collect in a responsible and lawful manner.

关于管理收集、使用和泄露个人信息的《2012年个人信息保护法》中有关信息保护的条款，已于2014年7月2日生效执行。**国际眼科专科中心新加坡私人有限公司 ("ISEC新加坡")** 将尽力对其收集的所有个人信息以妥善合法的途径进行处理。

By registering with **ISEC Singapore**, you consent to ISEC Singapore collecting, using, processing, and disclosing personal data about you solely in order to provide services to you, and for other related purposes including updating and maintaining our patient records, undertaking internal analysis for quality assurance, service improvement, management purposes, and other corporate business functions, making statutory returns, preventing crime, and complying with legal and regulatory requirements.

通过在**ISEC新加坡**进行登记，您已经同意**ISEC新加坡**仅为了向您提供服务、以及其他相关目的包括更新和维护我们的病人记录、针对质量保证实行内部分析、完善服务、加强管理和其他公司业务职能、回应监管部门需求、组织犯罪和遵守相关法律法规时，对您的个人信息进行收集、使用、处理和泄露。



Personal Data Protection Policy of ISEC Healthcare Ltd and its Affiliated Companies **Version 3.0**

If necessary, to administer your instructions, **ISEC Singapore** may share personal data about you with insurers and other medical practitioners.

如有需要，为了执行您的指使，**ISEC新加坡**可能会将您的个人信息与承保人和其他医护人员进行分享。

ISEC Singapore will keep confidential and secure all personal data about you.

ISEC新加坡将对您的 ([email address]) 进行绝对保密和安全。

If you have any questions about the personal data which **ISEC Singapore** holds, please contact our data protection officer at [email address].

如果您对于**ISEC新加坡**持有的个人信息有任何疑问，请以邮件方式与我们的数据保护执行官联系（邮箱地址为： [email address] ）。

Section 2 - Personal Data Collection Clause for Contracts and Consent Forms for Patients / Customers

[The following clause to be inserted in contracts / consent forms for patients.]

1. We may collect, use, process and disclose personal data about you (hereafter “**the personal data**”) solely in order to provide services to you, and for other related purposes including updating and maintaining our patient records, undertaking internal analysis for quality assurance, service improvement, management purposes, and other corporate business functions, making statutory returns, preventing crime, and complying with legal and regulatory requirements (the “**Specified Purposes**”).

为了向您提供服务、以及其他相关目的包括更新和维护我们的病人记录、针对质量保证实行内部分析、完善服务、加强管理和其他公司业务职能、回应监管部门需求、防止犯罪活动和遵守相关法律法规时（“**特殊目的**”），我们可能会对您的个人信息（下文统称“**个人信息**”）进行收集、使用、处理和泄露。

2. We agree to:

我们在此同意：

(a) collect, use, disclose, store or otherwise process the personal data for the Specified Purposes only and unless your written consent has first been

obtained, to not collect, use, disclose, store or otherwise process the personal data for other purposes or transfer the personal data out of Singapore;

只为了特殊目的对个人信息进行收集、使用、处理、保存或其他措施，除非事前得到您的书面同意，我们将不会为了其他目的对个人信息进行收集、使用、处理、保存或其他措施，也不会将个人信息转移到新加坡以外区域；

- (b) protect the personal data that you disclose to us with reasonable security arrangements to prevent the unauthorised access, collection, use, disclosure, copying, modification, transmission, distribution, disclosure, publication, disposal, destruction, deletion or other misuse, or loss or damage to the personal data so as to ensure the security and protection of the personal data;

采取合理有效的安全措施保护您透露给我们的个人信息，防止任何对于个人信息进行的非授权获取、收集、使用、披露、拷贝、复制、影印、传播、泄露、出版、处理、销毁、删除或其他不当使用、造成损害的行为，以确保对个人信息的保护；

- (c) upon your request in writing, return to you and not retain all records relating to or containing the personal data or any copies thereof, and erase your data from all forms of storage (including storage on back-up systems), save that we may retain such records and data if required by law, and provided that any such retention shall be in accordance with the Personal Data Protection Act 2012 and any applicable law; and

在收到您的书面要求后，将个人信息返还给您并不保留任何与个人信息有关的记录、或包含个人信息的复印件，并且从我们所有形式的数据库（包括备用系统）删除您的个人信息，但是如果应法律要求，我们会保留相应的个人信息，对于这类信息的保留将严格遵循2012年个人信息保护法和任何适用法律的要求；及

- (d) comply with all the requirements of the Personal Data Protection Act 2012 and any other relevant laws relating to the personal data.

遵守2012年个人信息保护法和任何其他与个人信息相关的法律的所有要求。

3. The personal data provided to us in connection with the Specified Purposes, whether stored in our servers or otherwise, shall be and shall remain your property.

您所提供给我们的与特殊目的相关的个人信息，无论是否存储在我们的数据库，均属于您的财产。



ANNEX C

**SAMPLE PERSONAL DATA COLLECTION CLAUSE
FOR JOB APPLICANTS**

Introduction

The following section of this Annex C sets out a sample personal data collection clause for use by ISEC in its job application forms.

Form of Clause

[The following clause to be inserted in the declaration section of job application forms.]

1. I consent to the collection, use, and disclosure of my personal data by ISEC Healthcare Ltd. and its related or affiliated companies for purposes that are related to or connected with my application, including, but not limited to, assessing my suitability for the position applied for, and obtaining employee references for background screening/vetting.
2. I represent and warrant that I have obtained the necessary consent from my family members to enable disclosure of their personal data for the purposes of my application.



ANNEX D

**SAMPLE PERSONAL DATA COLLECTION CLAUSE AND SUPPLEMENT
FOR EMPLOYEES**

Introduction

This Annex D sets out in Section 1, a personal data protection clause for use by ISEC in its new contracts of employment, and in Section 2, a supplement on personal data collection for use by ISEC in connection with existing contracts of employment.

Section 1 - Personal Data Collection Clause for New Contracts of Employment

[The following clause to be inserted in employment agreements and service agreements.]

1. You hereby consent to ISEC Healthcare Ltd. and its related or affiliated companies (collectively, "ISEC") collecting, using and disclosing your personal data for the purposes of administering and managing your employment relationship with ISEC; and these purposes include, but are not limited to:
 - (a) communicating with you;
 - (b) the provision of employment benefits (which include insurance, medical scheme, and other benefits from time to time); and
 - (c) providing employee references and for background screening or vetting.
2. You represent and warrant that you have obtained the necessary consent from your family members to enable collection, use and disclosure of their personal data by ISEC for the purposes of administering and managing your employment relationship with ISEC.
3. Notwithstanding the foregoing, you acknowledge that the Personal Data Protection Act 2012 ("PDPA") grants ISEC the right to collect, use and disclose your Personal Data without your consent for certain purposes that are related to or connected with your employment with the Company, and these purposes include, but are not limited, to:
 - (a) evaluative purposes;



Personal Data Protection Policy of ISEC Healthcare Ltd and its Affiliated Companies **Version 3.0**

- (b) for purposes of managing or terminating the employment relationship between you and ISEC; and
- (c) for purposes of a business asset transaction.

4. You agree that ISEC may disclose and transfer your Personal Data to:

- (a) its related or affiliated companies (collectively "**Related Companies**") for administering and managing the employment of all employees of ISEC and its Related Companies;
- (b) regulatory authorities and government agencies for purposes that are related to or connected with your employment with ISEC, or for purposes that may be required by law; and
- (c) third parties who provide products or services to ISEC or any of its Related Companies (such as professional advisers and payroll administrators) where it is necessary for the purposes of providing the products or services;

regardless whether the Related Companies, regulatory authorities, government agencies or third parties are located within or outside of Singapore provided that ISEC shall ensure that when disclosing or transferring your Personal Data to such an entity that the disclosure or transfer is only for the purposes set out in this clause and that the foreign entity has a standard of protection to your Personal Data that is comparable to the protection under the PDPA.

Section 2 - Supplement on Personal Data Collection for Existing Contracts of Employment

[The following Supplement to be printed on the letterhead of ISEC]

[Date]

[Name of Employee]

[Address]



Dear [Name of Employee],

PERSONAL DATA PROTECTION SUPPLEMENT TO EMPLOYMENT CONTRACT

1. This Supplement serves as a formal notice of changes to the terms and conditions of your Employment Contract. New provisions on personal data protection, as set out below, shall be added to your Employment Contract (where your Employment Contract does not already contain such similar provisions), or where your Employment Contract contains such similar provisions, such provisions shall be superseded by the following provisions on personal data protection.

Personal Data Protection

2. You hereby consent to ISEC Healthcare Ltd. and its related or affiliated companies (collectively, "ISEC") collecting, using and disclosing your personal data for the purposes of administering and managing your employment relationship with ISEC; and these purposes include, but are not limited to:
 - (a) communicating with you;
 - (b) the provision of employment benefits (which include insurance, medical scheme, and other benefits from time to time); and
 - (c) providing employee references and for background screening or vetting.
3. You represent and warrant that you have obtained the necessary consent from your family members to enable collection, use and disclosure of their personal data by ISEC for the purposes of administering and managing your employment relationship with ISEC.
4. Notwithstanding the foregoing, you acknowledge that the Personal Data Protection Act 2012 ("PDPA") grants ISEC the right to collect, use and disclose your Personal Data without your consent for certain purposes that are related to or connected with your employment with the Company, and these purposes include, but are not limited, to:
 - (a) evaluative purposes;



Personal Data Protection Policy of ISEC Healthcare Ltd and its Affiliated Companies **Version 3.0**

- (b) for purposes of managing or terminating the employment relationship between you and ISEC; and
- (c) for purposes of a business asset transaction.

5. You agree that ISEC may disclose and transfer your Personal Data to:

- (a) its related or affiliated companies (collectively "**Related Companies**") for administering and managing the employment of all employees of ISEC and its Related Companies;
- (b) regulatory authorities and government agencies for purposes that are related to or connected with your employment with ISEC, or for purposes that may be required by law; and
- (c) third parties who provide products or services to ISEC or any of its Related Companies (such as professional advisers and payroll administrators) where it is necessary for the purposes of providing the products or services;

regardless whether the Related Companies, regulatory authorities, government agencies or third parties are located within or outside of Singapore provided that ISEC shall ensure that when disclosing or transferring your Personal Data to such an entity that the disclosure or transfer is only for the purposes set out in this clause and that the foreign entity has a standard of protection to your Personal Data that is comparable to the protection under the PDPA.

General

- 6. Except as amended by this Supplement, all other terms and conditions of your Employment Contract shall remain in full force and effect. In the event of any conflict or inconsistency between the terms of this Supplement and your Employment Contract, the provisions of this Supplement shall prevail.
- 7. The invalidity, illegality or unenforceability of any provisions of this Supplement shall not affect the validity, legality or enforceability of any other provisions of this Supplement, provided that such invalid, illegal or unenforceable provision shall be



construed so as to give effect to the apparent and manifest intention of the Parties to the maximum extent allowed by law.

Effective Date and Entire Agreement

8. This Supplement shall come into effect from the date first above-written, and with effect from the same date, all references to your Employment Contract shall for all intents and purposes be deemed as references to your Employment Contract as amended and supplemented by, and read in conjunction with, this Supplement.
9. Your Employment Contract, as amended and supplemented by this Supplement, constitutes the entire agreement between the Parties relating to your employment and supersedes all prior agreements, or oral or written communications in connection with your employment.
10. This Supplement shall not be amended, changed, modified, supplemented or varied except by a written instrument signed by the Parties.

Governing Law

11. This Supplement shall be governed by and construed in accordance with the laws of Singapore and the Parties agree to submit any dispute arising from or in connection with this Supplement to the exclusive jurisdiction of the courts of Singapore.
12. Please sign the Acceptance and Acknowledgement section below to signify your agreement to the terms and conditions of this Supplement and return the same to us as soon as possible.

Yours sincerely,

ISEC Healthcare Ltd.

[Name], [Designation]

ACCEPTANCE AND ACKNOWLEDGEMENT



Personal Data Protection Policy of ISEC Healthcare Ltd and its Affiliated Companies ***Version 3.0***

To: **ISEC Healthcare Ltd.**

I have read and agree with the terms and conditions of the above Supplement and shall observe and comply with the terms of the Supplement.

Name:

NRIC / Passport No.:

Date:



ANNEX E

**SAMPLE PERSONAL DATA PROTECTION CLAUSE AND SUPPLEMENT
FOR THIRD PARTY CONTRACTS**

Introduction

This Annex E sets out in Section 1, a personal data protection clause for use by ISEC in new contracts with third party service providers / vendors, and in Section 2, a supplement on personal data protection for use by ISEC in connection with existing contracts with third party service providers / vendors.

Section 1 - Personal Data Protection Clause for New Contracts for Third Party Service Providers / Vendors

[The following clause to be inserted in new contracts with third party service providers / vendors.]

Personal Data Protection

1. In this Agreement:
 - (a) “**PDPA**” means the Personal Data Protection Act 2012 and shall include any amendment made thereto from time to time;
 - (b) “**Personal Data**” means any information relating to individual or individuals disclosed by ISEC to you, or collected by you pursuant to this Agreement; and
 - (c) “**processing**” has the meaning ascribed to it in the PDPA.
2. You agree to comply with the PDPA and all applicable laws and regulations relating in any way to the Personal Data, to the extent applicable to the provision by you of goods and services under this Agreement. You shall inform your employees having access to the Personal Data of the requirements set out in this Agreement.
3. You shall collect, use, process, and disclose Personal Data only on behalf of and for the benefit of ISEC and only to carry out your obligations under this Agreement to the extent required by ISEC’s written instructions. You shall treat all Personal Data as confidential subject to the confidentiality provisions in this Agreement. You shall not share, transfer, disclose or otherwise provide access to any Personal Data to any third party unless ISEC has authorised you to do so in writing. You shall take reasonable



Personal Data Protection Policy of ISEC Healthcare Ltd and its Affiliated Companies **Version 3.0**

steps to ensure that any Personal Data which you process is and remains complete and accurate.

4. To the extent that you are required to collect, use and disclose Singapore telephone numbers to send marketing messages in the course of carrying out your obligations under this Agreement, you shall, at your own cost and expense, fully comply with the requirements under Part IX, Do Not Call Registry, of the PDPA and such other laws, regulations and guidelines as may be issued by any regulatory authority or government agency from time to time, and with any directions that ISEC may give to you from time to time.
5. You shall not transfer the Personal Data outside of Singapore or other country/territory which ISEC or its personnel delivered it to you, as the case may be, without the prior written consent of ISEC. Where ISEC has given its written consent to such transfer, you shall ensure that the third party to whom the Personal Data is transferred shall provide a standard of protection to the Personal Data that is comparable to the protection under the PDPA and that the third party shall observe and comply with any conditions imposed by ISEC.
6. You shall take all reasonable measures to ensure that the Personal Data held by you is protected against loss, unauthorised access, use, modification, disclosure, and other misuse, and that only your authorised personnel have access to the Personal Data.
7. You shall employ administrative, physical and technical safeguards (including safeguards against worms, Trojan horses, and other disabling or damaging codes) to ensure that the Personal Data is afforded protection in accordance with the PDPA. You shall immediately inform ISEC in writing of any breaches of security that may result in the unauthorised collection, access, use or disclosure of the Personal Data.
8. You shall comply with any requests, directions or guidelines which ISEC may give to you from time to time arising in connection with the Personal Data.
9. If you subcontract any of your obligations under this Agreement subject to ISEC's prior written consent, you shall do so only by way of a written agreement with the sub-contractor which imposes the same level of protection for the Personal Data as imposed on you under this Agreement.
10. Promptly upon the expiration or earlier termination of this Agreement, or such earlier time as ISEC requests, you shall:
 - (a) cease to access, use or disclose any of the Personal Data (and shall ensure that your sub-contractors do likewise); and



- (b) return or, at ISEC's written instruction, destroy all Personal Data.
11. Notwithstanding and further to anything stated elsewhere in the Agreement, you:
- (a) undertake that should you commit any breach of its obligations in these personal data protection provisions, you shall do all that is within your powers to remedy the breach.
 - (b) acknowledge and agree that any breach of the undertakings set out in these personal data protection provisions could cause ISEC irreparable injury and that monetary damages would not be an adequate remedy for any such breach. In the event of a breach or threatened breach by you of any term set out in these personal data protection provisions, ISEC shall be entitled to injunctive relief in any court of competent jurisdiction restraining you from breaching the terms hereof or from disclosing any the Personal Data to any person.
 - (c) agree to indemnify ISEC for any costs, claims, demands or liabilities of whatsoever nature arising directly or indirectly out of a breach of your obligations in these personal data protection provisions. Nothing contained herein shall be construed as prohibiting ISEC from pursuing any other remedies available to ISEC, either at law or in equity, for such breach or threatened breach, including specific performance or other forms of equitable relief and recovery of monetary damages.

Section 2 - Supplement on Personal Data Protection for Existing Contracts with Third Party Service Providers / Vendors

[The following Supplement to be printed on the letterhead of ISEC.]

[Date]

[Name of Service Provider / Vendor]
[Address]

Attention: [Name of Contact Person]

Dear [Name of Contact Person],

SUPPLEMENT ON PERSONAL DATA PROTECTION



Personal Data Protection Policy of ISEC Healthcare Ltd and its Affiliated Companies Version 3.0

1. In order for ISEC Healthcare Ltd (“**ISEC**”) to comply with its obligations under the Personal Data Protection Act 2012 (“**PDPA**”), we require you as our vendor or third party service provider to observe and comply with the provisions set forth below on personal data protection.

Interpretation

2. In this Supplement, the following words and expressions have the meanings given to them below:
 - (a) “**Personal Data**” means any information relating to individual or individuals disclosed by ISEC to you, or collected by you in the course of the services which you have been engaged to perform or the provision of goods which you have been engaged to provide to ISEC (the “**Services**”); and
 - (b) “**processing**” has the meaning ascribed to it in the PDPA.
3. You agree to comply with the PDPA and all applicable laws and regulations relating in any way to the Personal Data, to the extent applicable to the provision by you of the Services. You shall inform your employees having access to the Personal Data of the requirements set out in this Supplement.
4. You shall collect, use, process, and disclose Personal Data only on behalf of and for the benefit of ISEC and only to carry out your obligations in the provision of the Services and to the extent required by ISEC’s written instructions. You shall treat all Personal Data as confidential subject to the confidentiality provisions in this Agreement. You shall not share, transfer, disclose or otherwise provide access to any Personal Data to any third party unless ISEC has authorised you to do so in writing. You shall take reasonable steps to ensure that any Personal Data which you process is and remains complete and accurate.
5. To the extent that you are required to collect, use and disclose Singapore telephone numbers to send marketing messages in the course of providing the Services, you shall, at your own cost and expense, fully comply with the requirements under Part IX, Do Not Call Registry, of the PDPA and such other laws, regulations and guidelines as may be issued by any regulatory authority or government agency from time to time, and with any directions that ISEC may give to you from time to time.
6. You shall not transfer the Personal Data outside of Singapore or other country/territory which ISEC or its personnel delivered it to you, as the case may be, without the prior written consent of ISEC. Where ISEC has given its written consent to such transfer, you shall ensure that the third party to whom the Personal Data is transferred shall

- provide a standard of protection to the Personal Data that is comparable to the protection under the PDPA and that the third party shall observe and comply with any conditions imposed by ISEC.
7. You shall take all reasonable measures to ensure that the Personal Data held by you is protected against loss, unauthorised access, use, modification, disclosure, and other misuse, and that only your authorised personnel have access to the Personal Data.
 8. You shall employ administrative, physical and technical safeguards (including safeguards against worms, Trojan horses, and other disabling or damaging codes) to ensure that the Personal Data is afforded protection in accordance with the PDPA. You shall immediately inform ISEC in writing of any breaches of security that may result in the unauthorised collection, access, use or disclosure of the Personal Data.
 9. You shall comply with any requests, directions or guidelines which ISEC may give to you from time to time arising in connection with the Personal Data.
 10. If you subcontract any of your obligations in the provision of the Services subject to ISEC's prior written consent, you shall do so only by way of a written agreement with the sub-contractor which imposes the same level of protection for the Personal Data as imposed on you under this Supplement.
 11. Promptly upon the expiration or earlier termination of the Services, or such earlier time as ISEC requests, you shall:
 - (a) cease to access, use or disclose any of the Personal Data (and shall ensure that your sub-contractors do likewise); and
 - (b) return or, at ISEC's written instruction, destroy all Personal Data.
 12. You undertake that should you commit any breach of its obligations in these personal data protection provisions, you shall do all that is within your powers to remedy the breach.
 13. You acknowledge and agree that any breach of the undertakings set out in these personal data protection provisions could cause ISEC irreparable injury and that monetary damages would not be an adequate remedy for any such breach. In the event of a breach or threatened breach by you of any term set out in these personal data protection provisions, ISEC shall be entitled to injunctive relief in any court of competent jurisdiction restraining you from breaching the terms hereof or from disclosing any the Personal Data to any person.



14. You agree to indemnify ISEC for any costs, claims, demands or liabilities of whatsoever nature arising directly or indirectly out of a breach of your obligations in these personal data protection provisions. Nothing contained herein shall be construed as prohibiting ISEC from pursuing any other remedies available to ISEC, either at law or in equity, for such breach or threatened breach, including specific performance or other forms of equitable relief and recovery of monetary damages.

General

15. Where there is in existence an Agreement signed by you for the provision of the Services, except as amended by this Supplement, all other terms and conditions of the Agreement shall remain in full force and effect. All references to the Agreement shall for all intents and purposes be deemed as references to the Agreement as amended and supplemented by, and read in conjunction with, this Supplement. In the event of any conflict or inconsistency between the terms of this Supplement and the Agreement, the provisions of this Supplement shall prevail.
16. The invalidity, illegality or unenforceability of any provisions of this Supplement shall not affect the validity, legality or enforceability of any other provisions of this Supplement, provided that such invalid, illegal or unenforceable provision shall be construed so as to give effect to the apparent and manifest intention of the Parties to the maximum extent allowed by law.

Effective Date and Entire Agreement

17. This Supplement shall come into effect from the date first above-written.
18. This Supplement constitutes the entire agreement between the Parties relating to the subject matter of this Supplement and supersedes all prior agreements, or oral or written communications in connection with the subject matter of this Supplement.
19. This Supplement shall not be amended, changed, modified, supplemented or varied except by a written instrument signed by the Parties.

Governing Law

20. This Supplement shall be governed by and construed in accordance with the laws of Singapore and the Parties agree to submit any dispute arising from or in connection with this Supplement to the exclusive jurisdiction of the courts of Singapore.



Personal Data Protection Policy of ISEC Healthcare Ltd and its Affiliated Companies Version 3.0

21. Please sign the Acceptance and Acknowledgement section below to signify your agreement to the terms and conditions of this Supplement and return the signed Supplement to us as soon as possible.

Yours sincerely,

ISEC Healthcare Ltd.

[Name of Authorised Signatory]

ACCEPTANCE AND ACKNOWLEDGEMENT

To: ISEC Healthcare Ltd.










We, [Name of Service Provider / Vendor], have read and agree with the terms and conditions of the above Supplement and shall observe and comply with the terms of the Supplement.

Name:

Designation:

Date:

ANNEX F
PERSONAL DATA PROTECTION FORMS CREATED / IN USE

No.	Description	Document
1	ISEC Healthcare Ltd. Employee Supplemental PDPA	 ISEC Healthcare Employee PDPA.doc
2	ISEC Healthcare Ltd. Vendor Supplemental PDPA	 ISEC Healthcare Vendor PDPA Suppl
3	Temasek Medical Centre Notice at Counters	 PDPA - Notice at Counters.docx
4	Temasek Medical Centre Patient Consent Forms – Bukit Batok	 PDPA - Patient Consent Forms - BB.
5	Temasek Medical Centre Patient Consent Forms – Sembawang	 PDPA - Patient Consent Forms - SB
6	Temasek Medical Centre Patient Consent Forms – Woodlands	 PDPA - Patient Consent Forms - WL
7	Temasek Medical Centre Patient Consent Forms – Yew Tee	 PDPA - Patient Consent Forms - YT.
8	Temasek Medical Centre Vendor Supplemental PDPA	 PDPA - For Locums and Third Party Venc
9	Temasek Medical Centre Locum Payment Advice – PDPA	 Payment Advice - Locum (revised).doc

ANNEX G

LIST OF DPOS AND CONTACT DETAILS

Entity	DPO	Designation
ISEC Group – Overall	Daniel Lai	Senior IT Manager
ISEC Healthcare Ltd. ISEC Eye Pte. Ltd. International Specialist Eye Centre Pte. Ltd. ISEC Global Pte. Ltd.	Maggie Ge	Director of Operations
JL Medical (Bukit Batok) Pte. Ltd.	Germaine Choy	Senior Clinic Assistant
JL Medical (Sembawang) Pte. Ltd.	Serene Tee	Senior Clinic Assistant
JL Medical (Woodlands) Pte. Ltd.	Tay Adeline	Clinic Assistant
JL Medical (Yew Tee) Pte. Ltd.	Catherine Gan	Senior Clinic Assistant

Entity	E-Mail
Asia Pacific Eye Centre	contact@asiapacificeyecentre.com.sg
Temasek Medical Centre	tmcpdpa@isec.sg