APPENDIX – REQUIREMENTS REGARDING HANDLING OF DATA BREACHES

Section A - Background

1. Some examples of Data Breach are illustrated below:

   (a) Loss of physical means on which MOHH Personal Data is stored (collectively referred to as "**Storage Devices**"). Examples of such Storage Devices include computer notebooks, mobile devices such as mobile phones or tablets, data storage devices such as thumb drives, and paper records of MOHH Personal Data.

   (b) Unauthorised access or disclosure of MOHH Personal Data by employees of the Vendor / Service Provider.

   (c) Sending and/or disclosing of MOHH Personal Data to wrong recipients e.g. through email or to physical address.

   (d) Improper disposal of MOHH Personal Data.

   (e) Hacking of electronic Storage Devices.

   (f) Theft of Storage Devices.

   (g) Exploitation of errors or bugs in programming code of the Vendor's / Service Provider's websites and/or databases by unauthorised third parties resulting in unauthorised access of MOHH Personal Data.

Section B - Obligations

2. The Vendor / Service Provider agrees to handle Data Breaches in compliance with the relevant guidelines issued by the Personal Data Protection Commission ("**PDPC Guidelines**"), the relevant requirements set out in the policies relating to data breaches as may be issued by the Ministry of Health from time to time (the "**MOH Policies**"), and any and all policies, guidelines, notices and circulars relating to data breaches which MOHH may from time to time notify in writing to the Vendor / Service Provider ("**MOHH Circulars**"). The PDPC Guidelines have been taken in consideration in the drafting and implementation of the MOHH Circulars.

3. Parties also agree to comply with the requirements set out below in relation to the handling of Data Breaches. In the event of a conflict between the obligations set out below, the PDPC Guidelines applicable at the time of the Data Breach, and the MOH Policies applicable at the time of the Data Breach, the conflict shall be resolved in the following order of priority: (1) the MOH Policies; (2) the MOHH Circulars; (3) PDPC Guidelines; (4) the obligations set out below.

   (a) NOTIFICATION TO MOHH

   In the event that the Vendor / Service Provider is aware of a Data Breach in respect of MOHH Personal Data, the Vendor / Service Provider shall immediately notify MOHH.

   Such notification should be made to MOHH no later than twenty-four (24) hours from the time the Vendor / Service Provider first becomes aware of the Data Breach. The notification form template is provided in Annex A below. For the avoidance of doubt, MOHH reserves the right to amend the notification form template in Annex A from time to time PROVIDED ALWAYS that the notification form template complies with and is subject to the MOH Policies, including but not limited to the HealthTech Instruction Manual. Any amendments to the notification form template made by MOHH shall be notified in writing to the Vendor / Service Provider.

(b) CONTAINMENT OF DATA BREACH

The Vendor / Service Provider should take immediate steps to contain the Data Breach. This typically means that any further access to or disclosure of MOHH Personal Data affected by the Data Breach should be limited to authorised persons who need such access or disclosure to rectify or mitigate the Data Breach. Examples of steps which may be taken to contain the Data Breach include:

a) Shutting down and/or isolating the system(s) which was involved in the Data Breach; and
b) Stopping practices and processes that led to the Data Breach.

The Vendor / Service Provider shall notify MOHH as soon as practicable regarding the steps it has taken to contain the Data Breach.

(c) PROVIDING ASSISTANCE AND COOPERATION

The Vendor / Service Provider shall work closely with MOHH to remedy and mitigate the Data Breach and shall provide relevant updates to MOHH regarding its response to the Data Breach as soon as practicable.

The Vendor / Service Provider shall also provide all necessary assistance and cooperation to MOHH in relation to any investigation of the Data Breach conducted by MOHH and/or any claim, allegation, action, proceeding or litigation involving MOHH which arises out of or in connection with the Data Breach.

(d) EVALUATION AFTER RESOLUTION OF THE DATA BREACH

After the Data Breach has been resolved, the Vendor / Service Provider and MOHH shall share findings with one another regarding how to prevent future Data Breaches. Such findings may include:

(a) assessment of the need to implement or to continue with any remediation actions and/or correction actions;
(b) identification of areas of weakness and the actions needed to strengthen such areas; and
(c) assessment of the effectiveness of the response(s) to the Data Breach.

Annex A – Data Breach Notification Form template

IMPORTANT NOTE: Please ensure that the completed form is submitted via email to the Data Protection Officer(s) of MOHH at the following email address: mohh.dpo@mohh.com.sg.

Report Date:	Report Time:
Notifying Party:	

1. Particulars of representative of Notifying Party ("Reporter")	
Name:	Designation:
Telephone No:	Department / Division:
Email Address:	
2. Details of Data Breach Incident	
Date Noted: (observation)	Time Noted:
Date Occurred: (earliest known occurrence)	Time Occurred:

Description of Incident:

Section A – Critical Information regarding the Incident

*Instructions: Please provide answers to **all** of the following questions in order for the Affected Parties to conduct their initial assessment of the risks arising from the Incident.*

(i) What was the cause(s) / suspected cause(s) of the Data Breach? *(Please refer to paragraph 2 of the Appendix for examples of possible causes, and provide as much information as possible regarding the cause(s) / suspected cause(s)).*

(ii) Is the Data Breach still ongoing?

(iii) How many individuals were affected by this Incident?

(iv) What types of MOHH Personal Data was involved in this Incident? Please indicate all data fields exposed as a result of this Incident.

(v) Were any MOHH Platforms affected by the Incident? If so, please indicate which MOHH Platforms were affected.

Section B – Other relevant information regarding the Incident

Instructions: Please provide answers to as many of the following questions as possible.

(vi) Who was / were the recipient(s) of the data involved in the data breach incident?

(vii) Were there any consequences and / or impact on the affected individuals? If so, do elaborate them here.

(viii) Were there any consequences and / or impact on MOHH? If so, do elaborate them here.

(ix) Were there any efforts taken by the Vendor / Service Provider to contain and investigate the incident? If so, do elaborate them here.