PERSONAL UNDERTAKING: MOHH Group Policy on Data Protection and Data Security

Patient confidentiality is a core value of the MOHH Group of companies ("**the Group**"). You play an important role in safeguarding the confidentiality of Group Information (as defined below) which you encounter in the course of your work.

It is important for you to note the following:

WHAT YOU MUST DO & WHAT YOU CANNOT DO

1. You must comply with all applicable laws, statutes, subsidiary legislation, rules, guidelines regarding legal and regulatory compliance from any relevant authority and any contractual obligations that protect the confidentiality of information owned by the Group, information which the Group handles on behalf of another party as an agent, data intermediary or collaborator, personal data (as defined in the Personal Data Protection Act 2012) and de-identified individualised datasets ("**Group Information**"). Group information may include the Group's internal circulars or policies, MOH's or other regulatory authorities' circulars or policies as may be applicable, and legal and financial documents such as contracts and financial statements, research findings, etc. Personal data typically refers to records of patients, staff, contractors and other individuals, such as name, NRIC, health records, income data, etc. De-identified records of individuals may form part of Group Information under non-disclosure obligations and may also be re-identifiable.

2. You must abide by all governing policies, practices and guidelines issued, amended and supplemented from time to time, by the MOH, MOHH and the MOHH Group entity which you are employed under, appointed, attached or seconded to, or render services to, which include: (i) data and IT security policies set out in the HealthTech Instruction Manual and other directives and circulars; and (ii) NHG policies on data protection and data security as listed in **Annex A**.

3. At any time **during and/or after** your employment / posting / appointment / training / attachment / internship / secondment ("**Employment**") with us and/or any other entity within the Group ("**Company**"):--

   a) you must ensure that the confidentiality of the Group Information is strictly maintained at all times and use the Group Information only for authorised purposes and do not divulge any Group Information to any unauthorised person;

b) you must understand that Group Information is made available to you purely to enable you to perform all duties assigned to you by us or a Company ("**Assigned Duties"**);

c) you must not access, copy, reproduce or use any Group Information for any unauthorised purpose;

d) unless you have proper authorisation to do so, you must not at any time:

(i) remove any documents or any other items containing Group Information from any of the Group's premises;

(ii) capture or publish on social media or any public electronic platform, the image or audio of any persons, documents, materials, events, incidents or equipment constituting or containing Group Information or on matters concerning any Group Information (whether conveyed formally or otherwise);

(iii) communicate to any external parties and/or organisations (including but not limited to business contacts, media, competitors, external authorities, etc.) on matters concerning any Group Information (whether conveyed formally or otherwise); or

(iv) attempt to re-identify, or disclose the method to re-identify the information or material, if you process or are given access to de-identified individualised data.

e) at all times, you must be vigilant in the disclosure of Group Information and ensure that the disclosures are authorised and compliant with security safeguards;

f) you must promptly return all Group Information and ensure no part or copies remain in your possession upon termination or expiration of the Purpose, and/or abide by any direction we may give for its proper disposition;

g) you must only access IT systems which you have been authorised to access for the Purpose only and for no other purpose, and you must not attempt to exceed the access levels given to you;

h) you must observe and abide by all terms and conditions that relate to the use of our IT systems that you are authorised to use;

i) after accessing these IT systems and after use, you must log off from your account;

j) you must not share or reveal any log-in identification or password assigned to you with anyone or allow it to be accessible to anyone;

k) if you inadvertently receive access to any information not normally received during the course of your Assigned Duties, you must notify your supervisor immediately and comply with their directions; and

l) you must notify your supervisors immediately if you become aware of any potential or actual breach of confidentiality of Group Information.

WHAT YOU SHOULD KNOW

4. A failure to observe confidentiality of Group Information is a breach of the terms and conditions of your Employment with us. You may be subject to internal disciplinary action, including termination of your Employment.

5. A failure to comply with the Group's policies, terms and conditions for the use and access of IT systems, contractual obligations and/or applicable laws, may also render you liable to disciplinary action and legal action in the event of a data breach, and termination of access to Group Information.

6. In addition, some breaches of confidentiality may also render you liable to criminal prosecution under the applicable laws, statutes and relevant subsidiary legislation.

7. Please note that your work emails and file uploads to the Internet will be monitored via Data Loss Prevention tools, in accordance with the NHG Data Loss Prevention Policy.

I have read and fully understood the MOHH Group Policy on Data Protection and Data Security. I undertake to ensure full compliance with this Undertaking.

RESPONSE SLIP

I have read and fully understood the MOHH Group Policy on Data Protection and Data Security. I undertake to ensure full compliance with this Undertaking.

Name: Dhammananda Justin Yu

NRIC: M0461528R

Signature[1]: 

Date: 2 October 2025

[1] Electronic authentication of person's identity and acceptance of Undertaking is permissible.