MINISTRY OF HEALTH
SINGAPORE

MH 6:01/5 MOH Circular No. 105/2021

06 August 2021

All PHMC-licensed Institutions

HEALTHCARE CYBERSECURITY ESSENTIALS (HCSE)

In the Ministry of Health (MOH)'s Cybersecurity Advisory to all licensees under the Private Hospitals and Medical Clinics Act (PHMCA) on 8 Feb 2021, MOH shared a set of cybersecurity measures in response to the SolarWinds supply chain attack to safeguard and ensure the integrity of personal and medical data within medical records, so as to be compliant with the PHMC Regulations and the Personal Data Protection Act (PDPA). MOH also indicated that we will be releasing a set of guidance to help licensees improve the cybersecurity of their IT systems.

2. MOH has since developed a set of Healthcare Cybersecurity Essentials (Annex A) with input from healthcare service providers, and which are meant as a 'guidance document' for licensees in adopting basic safeguards for their IT assets and data. HCSE has been designed to take into account implementation feasibility and is pitched at the baseline cyber hygiene for licensees with a small IT setup.

3. HCSE sets out twelve (12) recommendations which can be implemented in three steps ('**CSI**'):

a) Step 1: **C**reate IT asset inventory
b) Step 2: **S**ecure data, detect, respond to, and recover from breaches with technical, people and process measures
c) Step 3: **I**mplement by putting measures into practice

4. The recommendations under HCSE are broadly structured into three sub-sections: (i) explain the rationale and importance of the recommendations contextualised to the healthcare environment ("Why is it important?"); (ii) set out concrete action licensees can take ("What can you do?"); and (iii) suggest what larger or more well-resourced licensees can do to further improve their cybersecurity posture (Additional Tips).

Implementation

5. While HCSE is non-enforceable, we strongly encourage licensees to progressively implement all the measures and make the necessary changes to your current processes to safeguard your endpoints and IT systems. We encourage licensees to come onboard this cybersecurity journey early as the measures may potentially be translated to enforceable standards in future.

6. MOH recognises that some licensees may require additional support to adopt the recommendations under HCSE. For eligible licensees[1], you are encouraged to adopt the Infocomm Media Development Authority (IMDA)'s pre-approved cybersecurity solutions under the existing Productivity Solutions Grant (PSG) that may meet your need. We are also planning to roll out other implementation support in the coming months to support licensees in doing so. Further details will be shared once ready.

7. In the meantime, licensees may refer to these resources:

a) Dedicated cybersecurity webpage *at https://www.moh.gov.sg/licensing-and-regulation/cybersecurity-for-healthcare-providers* which provides information on HCSE, common signs of cyber-attacks, and latest announcements on the implementation support.

b) Policy template at *https://www.moh.gov.sg/docs/librariesprovider5/hrg-cybersecurity/policy-template.pdf* which can be adapted to help licensees in translating HCSE into actionable policies and processes relevant for your practice.

8. We look forward to your feedback regarding HCSE and support required in order to successfully implement the measures in HCSE via eLIS@moh.gov.sg.

ADJ ASSOC PROF (DR) RAYMOND CHUA
DEPUTY DIRECTOR OF MEDICAL SERVICES (HEALTH REGULATION GROUP)
& ASSISTANT COMMISSIONER (CYBERSECURITY)
MINISTRY OF HEALTH

MR LIONEL LEE
MINISTRY CHIEF INFORMATION SECURITY OFFICER
MINISTRY OF HEALTH

[1] You may visit https://www.enterprisesg.gov.sg/financial-assistance/grants/for-local-companies/productivity-solutions-grant/psg-faqs for more details on the eligibility criteria for PSG.