MINISTRY OF HEALTH
SINGAPORE

MH 6:01/5 MOH Circular No. 85/2023

4 Dec 2023

All PHMC/HCSA-licensed institutions, approved NEHR users, MOH entities, and community partners

CYBER & DATA SECURITY GUIDELINES FOR HEALTHCARE PROVIDERS

BACKGROUND

1. With increasing digitalisation, cyber-attacks and data breaches have become key risks for organisations and enterprises. In healthcare, such risks are heightened given that security breaches related to health information can potentially impact patient safety and care quality, beyond patient privacy and confidentiality. Further, such breaches are also extremely costly to organisations where it involves directly patching the affected systems and recovering lost data, or indirectly from reputational damage.

2. To better safeguard patients and support care continuity, the Ministry of Health (MOH) plans to introduce the Health Information Bill ("HIB") in mid-2024 to govern the safe and secure collection, access, use, and sharing of health information to enhance quality and continuity of care for patients. **Health information includes both administrative and clinical data where:**

i. **"Administrative data"** refers to any personal information that is related to the use or consumption of any healthcare service or community health service, and the provision of any healthcare service or community health service to an individual. Examples of "administrative data" include data such as demographics, contact details, and service utilisation information; and

ii. **"Clinical data"** refers to information about or relating to either or both of the following, in relation to an individual:
   a. Physical and mental health of an individual.
   b. Diagnosis, treatment, and care of an individual.

Ministry of Health, Singapore
College of Medicine Building
16 College Road
Singapore 169854
TEL (65) 6325 9220
FAX (65) 6224 1677
WEB www.moh.gov.sg

3. In conjunction, the **Cyber & Data Security Guidelines for Healthcare Providers** (**"Guidelines"**) were developed in consultation with the Cybersecurity Agency of Singapore (CSA), Infocomm Media Development Authority (IMDA), and Personal Data Protection Commission (PDPC), and build on the Healthcare Cybersecurity Essentials (HCSE) previously published on 6 August 2021. These Guidelines provide guidance on the cyber and data security measures to be put in place for the proper storage, access, use and sharing of health information in order to improve the security posture amongst healthcare providers[1], in the lead up to the implementation of the HIB. The HIB will require healthcare providers to meet cyber and data security requirements in order to contribute and / or access the National Electronic Health Record (NEHR) safely.

4. The Guidelines (**Annex A**) aim to provide clarity to healthcare providers on the requirements to secure the confidentiality, integrity, and availability of health information against unauthorised access, inappropriate modification, use, disclosure, disposal, or other similar risks. The key cyber and data security aspects of the Guidelines are detailed in **Table 1**.

Table 1: Key Cyber & Data Security Aspects under the Guidelines

Cybersecurity
Updates – *software updates* • Install software updates on your devices and systems promptly.
Secure/Protect – *virus/malware protection, access control, secure configuration* • Use anti-malware and anti-virus solutions to protect against malicious software. • Implement access control measures to control access to your data and services. • Use secure settings for your organisation's procured hardware & software.
Backup – *back up essential data* • Back up essential data and store them offline.
Asset – *people, hardware & software, data* • Equip staff with cyber-hygiene practices as the first line of defence. • Identify the hardware and software used in your organisation, and protect them. • Identify the type of data your organisation has, where they are stored, and secure them.

[1] Healthcare providers who will be designated as HIB entities include: i) Healthcare Services Act (HCSA) licensees; ii) Approved NEHR users (e.g., retail pharmacies); ii) MOH entities including MOH, MOH Office for Healthcare Transformation (MOHT), 2 Statutory Boards (Health Promotion Board and Health Sciences Authority), MOH Holdings and its entities (Agency of Integrated Care, ALPS) and the 3 public healthcare clusters (National University Health System / SingHealth / National Healthcare Group); and iv) relevant community partners (e.g., community care organisations).

Ministry of Health, Singapore
College of Medicine Building
16 College Road
Singapore 169854
TEL (65) 6325 9220
FAX (65) 6224 1677
WEB www.moh.gov.sg

Data Security
Secure – *storage, reproduction, and conveyance requirements* • Store your health information securely to prevent unauthorised access. • Do not reproduce copies of sensitive health information unless necessary. • Transport health information properly to avoid unwanted data exposure
Identify – *data security classification, marking requirements* • Know the information sensitivity levels of the data to apply appropriate safeguards. • Differentiate data of varying information sensitivity levels by marking their classification.
Access – *authorised users* • Restrict access to health information for valid and relevant purposes.
Common Cyber & Data Requirements
Outsourcing & Vendor Management • Understand the responsibilities set between your organisation and vendor.
Incident Response • Prepared to detect, respond, and recover from incidents.
Disposal Requirements • Proper disposal of health information mitigates the risk of unauthorised access.
Emergency Planning for Contingency • Supports ability to withstand service disruptions to ensure business continuity.
Review **S**ecurity & Internal Audit Requirements • Regular checks on corporate policies and processes to ensure compliance and identify vulnerabilities.

PLANNED IMPLEMENTATION

5. While the cyber and data security requirements are currently issued as Guidelines to promote early awareness and familiarity amongst healthcare providers, the requirements will eventually be imposed as regulatory requirements under the HIB. The exact timeline for the phased implementation of the requirements will be announced in future, with adequate sunrise period to be provided, taking into account: i) sectoral readiness and prevailing capabilities, ii) availability of implementation support plans to uplift cyber and data security posture, and iii) when mandatory data contribution to the NEHR will be enforced.

6. Following the issuance of the Guidelines, we will also be surveying healthcare providers in the coming quarter, to better i) profile their IT set-up, resourcing, and capabilities, and ii) understand their current cyber and data security readiness, which will help inform subsequent steps which MOH may take to support healthcare providers in preparing for HIB's eventual implementation.

7. For more information and resources, healthcare providers may refer to https://www.moh.gov.sg/licensing-and-regulation/cybersecurity-for-healthcare providers which provides information on the Guidelines, common signs of cyber-attacks or data breaches, and latest announcements on the implementation support.

8. We thank you and look forward to your feedback on the Guidelines which you may submit via go.gov.sg/cyber-data-guidelines-feedback. For any HIB-related enquiries, please email HIA_Enquiries@moh.gov.sg.

ADJ A/PROF (DR) RAYMOND CHUA
DEPUTY DIRECTOR-GENERAL OF HEALTH
HEALTH REGULATION
MINISTRY OF HEALTH

Annex

Annex A: Cyber & Data Security Guidelines for Healthcare Providers	*< Note: Please refer to the accompanying PDF document for this circular.>*

Ministry of Health, Singapore
College of Medicine Building
16 College Road
Singapore 169854
TEL (65) 6325 9220
FAX (65) 6224 1677
WEB www.moh.gov.sg