MINISTRY OF HEALTH
SINGAPORE

MH 78:60/1 MOH-MHA-0010-2026

16 November 2026

All HCSA Licensees

ADVISORY ON CYBERSECURITY AND DATA SECURITY

The Cyber Security Agency of Singapore (CSA) has highlighted a global surge in artificial intelligence-enabled cyberattacks, exploitation of vulnerable cyber-physical systems, and the mass exploitation of vulnerabilities in widely used software. Cyber incidents involving unauthorised access to systems, exposure of personal data and ransomware continue to affect organisations across sectors and of all sizes.

2. There have also been several recent cybersecurity incidents involving unauthorised access to the systems of healthcare and healthcare-related entities. The Ministry of Health (MOH) issued a statement about this on 12 November 2026.

3. MOH and the Health Sciences Authority (HSA) work with healthcare providers to safeguard our patients' health information. In view of the evolving threat landscape, we are issuing this advisory to urge all healthcare providers to remain vigilant, review their cybersecurity and data security preparedness, and take appropriate measures to strengthen their defences.

TAKE STEPS NOW TO STRENGTHEN YOUR DEFENCES

4. All healthcare providers are strongly encouraged to review their cybersecurity and data security arrangements and take appropriate precautionary measures as follow:

a) Keep your systems and software up to date

- Install software updates and security patches promptly, prioritising internet-facing servers.

b) Review remote and third-party access

- Identify remote and third-party access to your systems and ensure that such access remains necessary and appropriately secured.

c) Look out for signs of unauthorised activity

- Monitor for suspicious logins and unexpected changes to systems or data.

d) Review your incident response arrangements

- Verify that incident response contacts and escalation procedures are current.

e) Ensure that backups are usable

- Maintain offline, immutable backups, and test restoration periodically to ensure that they can be relied upon following an incident.

5. To prepare for the promulgation of the Health Information Act (HIA) which will be rolled out in phases from January 2027, healthcare providers may refer to MOH's Cybersecurity and Data Security (CS/DS) Essentials for the security measures and the HIA Implementation Guide for practical guidance on putting the measures in place.

STAY ALERT AND BE PREPARED TO RESPOND

6. Everyone has a role to play in protecting health information. Remind staff to exercise care when opening emails, clicking on links or accessing attachments, as phishing attempts are increasingly convincing and may be AI-assisted. Promptly report suspicious emails or unusual activity through your organisation's established channels.

7. If a cybersecurity or data security incident is suspected, activate your organisation's incident response processes promptly, seek appropriate technical assistance, and assess whether the incident needs to be reported to the relevant authorities in accordance with prevailing notification requirements. For MOHH entities, please follow the notification requirements in accordance with MOH's operations instruction for incident management and reporting (MOH-MHC-0054-2026 dated 7 July 2026). For non-MOHH entities, please escalate these incidents to MOH/HSA at HIA_Incidents@hsa.gov.sg and the Personal Data Protection Commission (PDPC) at https://eservice.pdpc.gov.sg/case/db.

FURTHER SUPPORT: CYBERSECURITY AND DATA SECURITY CONTINUING EDUCATION SESSION

8. MOH and HSA is organising a Cybersecurity and Data Security Continuing Education Session on 1 December 2026, 4-5pm. The session will cover current cyber threat landscape for the healthcare sector and share practical guidance on how healthcare providers can strengthen their cyber defences, stay alert to cybersecurity threats and respond to a cybersecurity/data security incident. There will also be an opportunity to hear from relevant experts and raise questions.

9. We strongly encourage licensees, managers and staff responsible for IT, operations and data protection to attend. Please register your interest here.

10. Cybersecurity is a shared responsibility. We encourage all healthcare providers to remain vigilant, review their cybersecurity preparedness and take proactive steps to safeguard their systems and information.

Mr COLIN LIM
CHIEF INFORMATION OFFICER AND GROUP DIRECTOR, INFOCOMM TECHNOLOGY AND DATA GROUP
MINISTRY OF HEALTH

Dr GOH KHEAN TEIK
GROUP DIRECTOR, HEALTH SERVICES GROUP
MINISTRY OF HEALTH