MINISTRY OF HEALTH
SINGAPORE

MH 6:01/5 MOH-MHA-0011-2026

16 November 2026

All Healthcare Information Management System (HIMS) Providers

STRENGTHENING CYBERSECURITY POSTURE FOR HEALTHCARE INFORMATION MANAGEMENT SYSTEMS (HIMS)

There have been several recent cybersecurity incidents involving unauthorised access to the systems of healthcare and healthcare-related entities. To our knowledge, there had not been unauthorised access of patient health records in these breaches. Nevertheless, the Ministry of Health (MOH) is taking these incidents very seriously and is following up with the affected entities to check on the full implications from these incidents.

2. The recent incidents serve as a timely reminder of the need for continued vigilance. As highlighted in MOH's press statement of 12 November 2026, healthcare institutions and HIMS providers should remain vigilant to evolving cyber threats. With advances in technology, particularly AI, vulnerabilities can be identified and exploited more readily, while cyberattacks are becoming increasingly frequent, rapid and sophisticated. Healthcare institutions and HIMS providers should therefore strengthen their cybersecurity posture and ensure the security and integrity of their IT assets, systems and patient data.

3. This advisory outlines key cybersecurity measures for the secure management of internet-facing applications, services and Application Programming Interfaces[1] (APIs), to reduce potential attack surfaces and strengthen overall system security, as observed from recent cyber and data breach incidents affecting healthcare organisations.

Strengthening Security Controls

4. HIMS providers are required to conduct an immediate and comprehensive review of their cybersecurity posture and take appropriate measures to identify, assess and mitigate cybersecurity risks within their systems and supporting infrastructure. In

[1] Application Programming Interfaces (APIs) refer to standardised and secure digital interfaces that enable authorised systems and applications to electronically exchange data, access services, and interoperate with one another through defined protocols and specifications.

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

particular, HIMS providers should review the following areas and address any identified gaps in a timely manner:

A. Review and Minimise Exposure of Internet-Facing Applications and APIs

5. HIMS providers are required to conduct a review of their internet-facing applications, services and APIs and take appropriate measures to minimise unnecessary exposure to the Internet. Access should be restricted to authorised users, systems and network locations, and providers should maintain an up-to-date inventory of externally accessible systems, interfaces and connections. Appropriate authentication measures, including multi-factor authentication for privileged and administrative access, should be implemented where applicable. APIs intended solely for internal system-to-system communications should not be publicly accessible from the Internet.

B. Assess and Remediate API Vulnerabilities

6. HIMS providers are expected to conduct regular security assessments of internet-facing applications, services and APIs to identify vulnerabilities and security weaknesses. Identified vulnerabilities should be assessed, prioritised and remediated in a timely manner, with appropriate testing performed to verify the effectiveness of remediation measures. Providers should maintain records of assessment and remediation activities as part of their security management processes.

C. Enhance Security Monitoring and Threat Detection

7. HIMS providers are required to establish appropriate monitoring and detection capabilities to identify suspicious activities, unauthorised access attempts and potential cybersecurity incidents affecting their systems. Relevant logs should be maintained and regularly reviewed, and identified security events should be investigated and responded to in a timely manner.

D. Assess Downstream and Third-Party Risks

8. HIMS providers are expected to assess risks arising from interconnected systems, third-party services and external dependencies, and implement appropriate measures to mitigate identified risks. Where remediation cannot be completed immediately, suitable mitigating controls should be implemented until the risks are adequately addressed.

Reporting and Accountability

9. Any API vulnerabilities, suspicious activities, or cybersecurity incidents affecting organisational systems shall be reported promptly through established incident reporting channels, with critical vulnerabilities or active exploitation escalated immediately to relevant cybersecurity and management stakeholders. HIMS Providers remain responsible for conducting the necessary reviews, remediating vulnerabilities in a timely manner, managing residual risks, and maintaining records of all review,

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

remediation, and risk treatment activities for audit, compliance, and assurance purposes. Refer to Annex A3 (ii) for incident assessment and reporting requirements.

10. The Health Information Act (HIA) governs Cybersecurity and Data Security (CS/DS) Measures where licensed healthcare providers, retail pharmacies, approved users of the NEHR, and Health Information Management System (HIMS) providers must implement reasonable security measures to protect health information and systems and meet cybersecurity incidents / data breach notification obligations. In preparation for the phased rollout of the HIA from January 2027, HIMS providers are reminded of their obligations under the HIA, including:

a) Cybersecurity and Data Security (CS/DS) Requirements: HIMS providing their services for healthcare providers must ensure that the confidentiality, integrity and availability of the health information are protected at all times.

b) Incident Management: HIMS providers will need to notify healthcare providers in the event of cyber security incidents and / or data breaches. Where a cybersecurity incident and / or data breach is clearly attributed to the vulnerabilities of a HIMS being exploited by threat actors, both the healthcare provider and the HIMS provider may be investigated, and enforcement action may be taken based on the facts of the case.

11. In addition, HIMS providers should note the joint advisory issued by the Personal Data Protection Commission (PDPC) and the Cyber Security Agency of Singapore (CSA) on 12 November 2026 on data protection risks arising from insecure APIs. HIMS providers should review the advisory and implement the recommended security measures to mitigate API-related vulnerabilities and reduce the risk of unauthorised access, data breaches, and service disruptions.

12. Refer to Annex A for key cybersecurity and data security resources. Should you require any further information or clarification, please email us at HIA_Enquiries@hsa.gov.sg.

MR COLIN LIM
CHIEF INFORMATION & CHIEF DATA OFFICER
MINISTRY OF HEALTH

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

Annex A: Key cybersecurity and data security resources.

Ref	Resources	Website QR Code
A1	MOH Press Releases on 12 November 2026 **STATEMENT ON RECENT CYBERSECURITY INCIDENTS IN HEALTHCARE SECTOR**	
A2	CSA Advisories on 12 November 2026 **Joint Advisory on Data Protection Risks Arising from Insecure APIs by the Personal Data Protection Commission and Cyber Security Agency of Singapore**	
A3	**About Cybersecurity and Data Security (CS/DS)** i. Cybersecurity & Data Security Essentials ii. Incident Assessment and Reporting, including HIA Implementation Guide iii. Compliance, Liability, and Enforcement	
A4	**Cyber Essentials for HIMS vendors Certification** (by Cyber Security Agency of Singapore) i. Certification document for Cyber Essentials ii. Self-assessment template	
A5	**OWASP API Security Project** Recommendation for API Security Top 10 2023 version	

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