MINISTRY OF HEALTH
SINGAPORE

REMEMBER YOUR 12 HEALTHCARE CYBERSECURITY ESSENTIALS

Amidst the constant and evolving cybersecurity threats, the Ministry of Health (MOH) has developed a set of basic 'Healthcare Cybersecurity Essentials' (HCSE) to better support healthcare providers to strengthen your cybersecurity posture at the endpoints and network environment. This will safeguard and ensure the integrity of the personal and medical data within the medical records as part of managing clinical risk and upholding patient safety.

Whom do HCSE apply to?

All healthcare providers licensed under the Private Hospitals and Medical Clinics Act (PHMCA) and the Healthcare Services Act (HCSA), as well as entities providing intermediate and long term care services.

Share the guidelines with persons in your organisation who have access to or manage data and systems, e.g. healthcare professional, IT staff, clinic assistant.

What do you need to do?

C Create IT asset inventory

S Secure data, detect, respond to, and recover from breaches

I Implement by putting measures into practice

MINISTRY OF HEALTH
SINGAPORE

Step 1: Create IT asset inventory

1. Create and maintain an updated inventory of all IT assets
Count and list all IT assets connected to the corporate IT network, including hardware, software, and medical devices with network connectivity.

Step 2: Secure data, detect, respond to, and recover from breaches

Technical

2. Restrict access rights according to the role of your staff

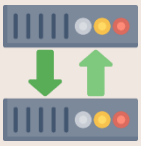
3. Choose systems with **multi-factor authentication** functionality

4. Update **security patches** regularly

5. Deploy **anti-malware** protection **(e.g. anti-virus)**

6. Secure your **network perimeter** (e.g. firewall)

7. Enable user **audit trail and security log**



8. Perform **regular backups** of all critical data and systems

Process

9. Develop **outsourcing policy** to screen and select vendors

10. Report data breaches promptly to mitigate impact

People

11. Raise **security awareness** among staff

Step 3: Implement by putting measures into practice

12. Review HCSE and translate them into **policies and processes** for your organisation

MINISTRY OF HEALTH
SINGAPORE

Tips: What are some signs that you have been attacked?

- Usual files, applications, or services cannot be accessed.
- Files have been unexpectedly encrypted, blocking your access to them.
- Accounts have been locked or the passwords changed without your knowledge.
- Software have been found to be unknowingly deleted or installed when compared against your IT asset inventory.
- Suspicious pop-ups load when you access the internet.
- Slower than normal internet speeds due to a spike in network traffic.

Tips: What should you do if you discover the signs that you have been attacked?

- If you have an IT vendor, contact them for assistance to find out the cause of the attack (e.g. system vulnerabilities) and impact (e.g. any data loss) to better understand the breach and to develop a recovery plan.
- Perform a security check on all affected systems accounts.
- Report the incident to the relevant authority:
  - For data breaches, notify the Personal Data Protection Commission at https://eservice.pdpc.gov.sg/case/db OR +65 3777 3131 during office hour for reported cases as required in Personal Data Protection Act.
  - For cyber-incidents, report to SingCERT via singcert@csa.gov.sg OR https://www.csa.gov.sg/singcert/reporting
  - Lodge a police report at https://eservices.police.gov.sg/ if you may have been a cybercrime victim

Let's All Do Our Part

Safeguarding Patient Records, Data, and Systems Is Everyone's Responsibility

Visit https://go.gov.sg/6amxrt for Healthcare Cybersecurity Essentials

Brought to you by:
Health Regulation Group &
Ministry Chief Information Security Officer's Office, MOH