MINISTRY OF HEALTH
SINGAPORE

HEALTHCARE CYBERSECURITY ESSENTIALS

Supported by Cyber Security Agency of Singapore (CSA)

August 2021

Contents

1. Introduction

1.1 Protecting patient's personal and medical data and maintaining its confidentiality, integrity and availability is an important part of managing clinical risk, enabling healthcare professionals to deliver accurate and appropriate care, and upholding patient safety. As healthcare providers embark on their digitalisation journey and continue to rely on technology to run their day-to-day operations, it is important to put in place measures to protect personal and medical data within electronic medical records.

1.2 Cyber-attacks are particularly threatening to the healthcare sector as healthcare providers handle and store patients' private information (such as medical records, contact information, financial and insurance details) that may be of value to data thieves in abusing such information for financial gain. Moreover, if records or systems parameters are maliciously altered, this may disrupt healthcare providers' ability to deliver appropriate patient care, resulting in harm to patients. Hence, cybersecurity is critical to the provision of quality and safe healthcare services in ensuring patient safety and welfare.

1.3 The rise in cyber incidents gives rise to a need to establish a set of baseline security standards for the healthcare industry. This document ('Healthcare Cybersecurity Essentials') aims to strengthen cybersecurity awareness by sensitising healthcare providers to and signaling the importance of cybersecurity as a critical part of clinical operations.

2. Objective and Scope

2.1 The objective of the Healthcare Cybersecurity Essentials (HCSE) is to provide guidance to all healthcare providers on basic cybersecurity measures that they can adopt to ensure the security and integrity of their IT assets, systems, and patient data. While the guidelines are presently **non-enforceable**, all healthcare providers are strongly encouraged to take steps to adopt the recommended measures within early.

2.2 It offers 12 key recommendations which healthcare providers can implement in three steps ('**CSI**')

- **Step 1: C**reate IT asset inventory
- **Step 2: S**ecure data, detect, respond to, and recover from breaches
- **Step 3: I**mplement by putting measures into practice

3. How to use these guidelines?

3.1 The recommendations under HCSE are broadly structured into three sub-sections: (i) "*Why is this important?*", which explains the rationale and importance for the recommendations which are contextualised to the healthcare environment; (ii) "*What should healthcare providers do?*", which sets out concrete actions healthcare providers can take; and (iii) *Tips*", which suggest additional actions the healthcare providers can do to further improve their cybersecurity posture.

4. Step 1: Create IT asset inventory

4.1 Why is this important?

4.1.1 Creating and maintaining an updated inventory of all IT assets enables healthcare providers to identify what they need to protect and detect unauthorised hardware or software in their network. Non-corporate devices (e.g. personal laptops or devices) may have security bugs which could be exploited or malware which may compromise them. Having only software which is needed for the clinical work and healthcare operations means that the providers may be exposed to fewer security bugs which could be exploited and have fewer software which needs to be kept up-to-date.

4.2 What should healthcare providers do?

4.2.1 For a start, healthcare providers should physically count and list all assets connected to the corporate IT network. This includes:

- Hardware such as PCs, laptops, printers, modems and network routers;
- Software such as clinical management and electronic medical records systems, accounting and HR software, Microsoft Word and Excel; and
- Medical Devices with network connectivity.

4.2.2 As part of IT asset management, healthcare providers should also:

- include the device name and the version information of each software, to aid subsequent work such as patching.
- update the asset inventory whenever there are any changes in hardware and software, such as new purchases, upgrades, or replacements.
- install only software which is needed on corporate devices. Disconnect any devices and uninstall any software that is no longer in use from the corporate IT network.
- use only corporate devices when accessing patient and corporate information.

Tips!

If healthcare providers want to do more, they can

- Review the asset inventory regularly (e.g. every quarter) and have a senior staff verify the inventory listing and count.
- Install and run software to:
    - help manage the asset inventory list/map.
    - automatically check that only authorised corporate assets are allowed to connect into the corporate IT network.
- Draw and maintain an architecture diagram (map) of the internal and external connections made by assets from the corporate network.

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

The recommendations under Step 2 covers areas ranging from technical, process and people aspects ("**TPP**").

5.1 Technical

a) Administrator and User Accounts Management

5.1.1 Why is it important?

(1) Most operating systems on computers provide 2 main types of user accounts:

- Administrator accounts – These accounts give their users rights to grant special permission, such as changing security settings, installing software and hardware, and accessing all files on the computer. Administrators can also make changes to other user accounts.
- User accounts – These accounts are for users who need to run applications but do not need to perform any of the above functions.

(2) As administrator accounts are 'keys to the kingdom' with elevated privileged access, they are commonly used by malicious attackers to compromise systems. An attacker using an administrative account can cause far more damage than one using a standard user account. For most day-to-day user activity such as entering clinical information into electronic medical records (EMR) and billing patients for consultation, administrative accounts are not required.

5.1.2 What should healthcare providers do?

(1) Healthcare providers should

- review the privileges required for all accounts and give users, other than the administrator, the least user privileges necessary to carry out his/her work. Staff with administrator privileges should only use their administrator account when required, and not when reading email or accessing external websites.
- review the privileges regularly according to the scope of the user in the institution.
- ensure that unused accounts are deleted as soon as possible and removed immediately once a user leaves the institution.
- investigate any suspicious use of dormant accounts.

Tips!

If healthcare providers want to do more, they can

- grant user account privileges according to what each staff requires to carry out his/her work. For example:

- A patient care associate should not require access to patients' clinical notes and investigation results.
- A nurse should not need to edit a patient's clinical notes.
- A network administrator should not require access to patient and corporate data.

- monitor all administrator accounts and ensure that their actions are verified or authorised.

b) Multi-Factor Authentication

5.1.3 Why is it important?

(1) Passwords are an easy target for hackers. Multi-factor authentication (MFA) requires users to submit at least two factors to prove their identity in order to gain access to a device or application. There are three categories of factors:

- Something you are: e.g. fingerprint, retina.
- Something you have: e.g. mobile device, physical token.
- Something you know: e.g. username and password.

(2) Requiring multiple factors makes it more difficult for an attacker to gain access. If one factor is compromised, the attacker still has at least one more barrier to breach before successfully breaking into the target.

5.1.4 What should healthcare providers do?

(1) Healthcare providers should

- choose systems with MFA functionality to manage and access patient and corporate information.
- configure all accounts in systems with MFA functionality such that a user gets access only if he/she has every authentication factor right
- ensure that staff do not share tokens or passwords. If any physical token is lost, it should be disabled immediately.

Tips!

If healthcare providers want to do more, they can

- ensure the second factor of authentication is performed through a separate communication channel e.g. using PC for first factor and mobile device for second factor.
- manage and audit the use of each authentication factor.

c) Security Patches

5.1.5 Why is it important?

(1) Manufacturers and developers release regular updates, or patches, which not only add new features, but also fix any security vulnerabilities that have been discovered. Any network connected system could be affected, including desktop and laptop computers; clinical, personnel or financial

information systems; databases containing sensitive digital health records and images; mobile devices; and medical equipment.

(2) Users should update their software regularly, otherwise attackers can use such flaws to break into corporate networks and steal data, or even cause malfunction of IT systems and medical devices and compromise patient care.

5.1.6 What should healthcare providers do?

(1) Healthcare providers should

- develop a plan for regular patching of all software and monitoring the progress of patching. It is important that updates are scheduled at a time that will not interfere with patient care. If there are any critical applications, healthcare providers should check with the software vendor if it will be able to support the latest security patches for the IT systems.
- avoid using software or hardware that is no longer supported by the manufacturer as security patches may not be available.
- develop a plan for removing any unsupported software and hardware and find replacements.
- only use updates from established software companies or legitimate sources.

Tips!

If healthcare providers want to do more, they can

- standardise the software used in the organisation to make updating more manageable, thereby reducing operating costs.
- manage the updating process centrally and consider using automated patch management solutions so that they can easily identify all the updated software, as well as outdated applications or operating systems.
- proactively prepare their organisation to use a new software from a vendor that offer support and service to inform customers when one of their software is about to or has reached the end of its lifespan.

d) Malware Protection

5.1.7 Why is it important?

(1) Just like a disease, malware (short for 'malicious software') is any program or file that infects a software and causes harm to the user. Types of malware can include computer viruses, worms, and spyware. Malware can perform a variety of functions such as stealing, encrypting or deleting sensitive patient data, or altering or hijacking core functions of machines such as causing medical devices to malfunction.

(2) One type of malware that is particularly common in the healthcare sector is ransomware. Ransomware prevents access to important healthcare data or causes malfunction of systems – clinical, personnel and financial information systems, databases containing health records, and medical devices – until the victim makes a payment. Depending on the access obtained, an attacker might also be able to read, modify, export and even publicly release digital health records.

(3) There are various ways in which malware can find its way onto a computer. A user may open an infected email attachment, browse a malicious website, or use a removable storage drive, such as a USB memory stick, which is carrying malware.

5.1.8 What should healthcare providers do?

(1) Healthcare providers should

- deploy anti-malware protection (e.g. anti-virus) for endpoints and update malware definitions as soon as they are available.
- configure anti-malware software to automatically scan any removable media (e.g. USBs, external hard drives and DVDs) when they are connected to computers.
- monitor and track all anti-malware alerts to ensure malware is quarantined and removed.

Tips!

If healthcare providers want to do more, they can

- install an application control solution that is integrated with antivirus software that uses both whitelisting and blacklisting approaches to prevent unauthorised applications including malware from running. The whitelist takes reference from the list of organisation's authorised assets.
- review the list of block applications from the application control solution and remove all unnecessary applications.
- deploy additional anti-malware protection measures depending on the set-up (e.g. anti-virus and spam filters for email servers, web content filtering and whitelisting of web domains for web proxy servers).

e) Network Perimeter Defence

5.1.9 Why is it important?

(1) It is likely that healthcare businesses require a connection to the Internet for day-to-day functions. Any network connected to the Internet is potentially within reach of attackers from anywhere in the world, and at risk of intrusion. Just as one secures his/her house from intruders with a fence and alarm system, network perimeter defences are necessary to prevent attackers

from intruding into the business network and stealing, modifying information or compromising systems.

5.1.10 What should healthcare providers do?

(1) There are many ways to secure the network perimeter. It is recommended that healthcare providers work with their IT vendors to ensure that they have one or more of the following in place, appropriate for their respective set-up:

- installing and configuring firewalls on endpoint devices (e.g. Windows Firewall).
- implementing controls at the network perimeter (e.g. firewalls, intrusion detection and prevention systems) to restrict unauthorised traffic if they have a local network.

f) Audit Logs

5.1.11 Why is it important?

(1) Audit trails show who has accessed the IT network or systems and what operations they have performed. Security logs show who has logged in and out of the system. Having such logs is critical to understanding the nature of security incidents during an active investigation and postmortem analysis. It is also useful to establish baseline and identify suspicious trends.

5.1.12 What should healthcare providers do?

(1) Healthcare providers should

- ensure that users' audit trails and security logging is enabled on all IT systems and devices or keep a manual log if this is not possible.
- maintain log-in rules properly and review them periodically.
- ensure that only authorised individuals have access to the security logs.
- constantly monitor and review audit trails and security logs to determine if systems have been breached; flag out possible inappropriate access or suspicious behavior to the heads of organisations.

> ***Tips!***
> If healthcare providers want to do more, they can roll out a centralised audit trail so that all security logs are consolidated in a separate location for easier monitoring and security.

g) Backups

5.1.13 Why is it important?

(1) A backup is a copy of the computer files which is stored separately from the computer or device. Hardware failure, theft, or malware infection

(especially ransomware, particularly common in healthcare) can make recovering critical data expensive or impossible. Furthermore, failure to back up critical data could jeopardise patient safety. Conversely, having a recent backup of the data will help the provider to recover more quickly.

5.1.14 What should healthcare providers do?

(1) Healthcare providers should

- consider all data they possess and identify critical data that would jeopardise patient safety and confidentiality, or adversely impact the practice if it was lost.
- perform frequent and regular backups of all critical data and systems.
    - Keep offline backups to protect against ransomware.
    - Keep offsite backups to protect against theft or natural disasters.
- test backups periodically to ensure they are usable during an emergency.
- ensure backups are also protected to prevent them from being compromised.

5.2 Process

a) Outsourcing and Vendor Management

5.2.1 Why is it important?

(1) Third-party software and devices are used extensively in healthcare settings, as healthcare providers do not typically design in-house software or devices. Third-party software and hardware can expose the systems to threats including the potential to compromise database integrity, open up security weaknesses that allow unauthorised access into the systems, and data breaches.

5.2.2 What should healthcare providers do?

(1) When using third party software and devices, healthcare providers should

- ensure that they clearly understand
    - how patient and corporate data is processed, transferred and stored.
    - the safeguards vendors have in place to secure the third-party software and devices they provide, including any assurance on activities carried out (e.g. certification, audits).
    - what the contractual arrangements with vendors are, including responsibilities in the event of an incident or breach.
- subscribe to security-related alerts published by vendors for the third-party software and devices their practice uses.

(2) If healthcare providers are using an IT service provider to manage their network and systems, they should

- clearly understand the services and security practices the IT service provider will provide.
- ask the IT service provider to provide regular vulnerability reports and updates about security issues for the systems they are managing on behalf of the healthcare provider.

(3) If healthcare providers are using cloud services, they should ensure the division of responsibilities for setting security configurations is clearly defined and understood.

b) Incident Reporting

5.2.3 Why is it important?

(1) A data breach occurs when personal information held by healthcare providers is lost or subjected to unauthorised access. Data breaches can occur:

- through unauthorised access to systems containing personal information;
- through intentional and inappropriate disclosure of personal information by staff; or
- through loss or theft of laptops, mobile devices, removable storage devices, and even paper records containing personal information.

(2) Reporting data breaches promptly facilitates incident response, mitigates the impact of the breach and upholds patient confidentiality.

5.2.4 What should healthcare providers do?

(1) The healthcare providers should ensure all staff are aware of how to report suspicious activity and possible incidents based on the obligations under prevailing legislative or regulatory requirements.

(2) The healthcare providers are strongly encouraged to report cyber incidents to SingCERT at https://www.csa.gov.sg/singcert/reporting. This includes

- Phishing, extortion, scam emails
- Phishing websites
- Ransomware attacks
- Website defacements
- Malware hosting/Command and Control Servers
- Unauthorised attempts (either failed or successful) to disrupt or gain access to a network, system or its data

(3) If the healthcare providers suspect that they may have been a victim of cybercrime, they should also lodge a police report at https://eservices.police.gov.sg/.

(4) In addition, healthcare providers are reminded of their reporting obligations under the Personal Data Protection Act (PDPA) to report data breach incidents at https://eservice.pdpc.gov.sg/case/db.

Tips!
If healthcare providers want to do more, they can form a dedicated incident response team (with trained personnel) to be the main point of contact for dealing with cybersecurity incidents in the organisation, including detection and mitigation of cybersecurity security incidents and restoration of organisation's functions.

5.3 People

a) Cybersecurity Awareness

5.3.1 Why is it important?

(1) Human error makes a significant difference in the delivery of healthcare services. Similarly, minimising human error is an essential part of a successful information security program. The busy and publicly accessible nature of many healthcare working environments makes cyber hygiene essential.

(2) It has been reported that users are responsible for detecting up to 95% of cyber incidents[1].There are many reasons why users may not always follow security practices. These include a lack of knowledge, perceived inconvenience, forgetfulness and not understanding the link between individual security behaviours and personal and organisational consequences. Cybersecurity awareness programmes could help to address these areas.

(3) One of the most prevalent types of cybercrime is phishing which targets the users' behaviour. It is a practice where attackers disguise themselves as a legitimate individual or reputable organisation in email, instant messaging and other communication channels to fraudulently obtain personal details and user credentials to gain access to networks or install malicious files to distribute trojan malware in the systems.

5.3.2 What should healthcare providers do?

(1) Healthcare providers should raise cybersecurity awareness among employees who access systems and data through suitable training and awareness programmes.

[1] IBM Security Services 2014 Cyber Security Intelligence Index

(2) Cybersecurity training and awareness programmes for employees should include information on the following as a baseline:

- Password Security – Encouraging the use of passphrases that combine at least four random words; not using the same password for multiple accounts; avoiding the use of publicly known information as passwords or writing down passwords and leaving them unprotected.
- Logging out and shutting down – Reminding users to always log out of applications and websites after use; locking computers when unattended; shutting down computers at the end of the day and clearing work areas of sensitive documents.
- Using trusted connections and sites – Helping users learn how to safely use public connections; recognising fake websites and phishing emails.
- Staying informed – Offering or participating in training to help users to continually update their skills and be aware of the risks of using online services; ensuring users know how to report any concerns; and explaining the personal consequences associated with sharing personal information during online interactions and on social media.
- Being aware – Encouraging users to look out for and report any suspicious behaviours.

6. Step 3: Implement by putting measures into practice

6.1 Why is it important?

(1) HCSE is designed as a set of baseline guidelines to help healthcare providers improve the security of their systems and data. To ensure these guidelines and other security policies are consistently applied throughout the organisation, it is important to translate them into policies and processes which all employees and vendors are required to be aware of and comply with.

6.2 What should healthcare providers do?

(1) Healthcare providers should

- review HCSE and translate them into policies and processes for their organisation.
- ensure that the policies and processes are endorsed by the head of the organisation or equivalent and communicated to all employees and vendors to ensure consistent understanding and practice.
- review the policies and processes regularly, and in particular, any updates to HCSE or guidance sent out by the authorities.

7. Contact Information

(1) For further clarification or information on HCSE, healthcare providers may wish to contact

- MOH via email at [eLIS@moh.gov.sg] if you are healthcare providers licensed under the Private Hospitals and Medical Clinics Act.
- AIC via email at [itsecurity@aic.sg] if you are healthcare providers in the ComCare sector or via email at [gp@chas.sg] if you are in the primary care sector.