MINISTRY OF HEALTH
SINGAPORE

CYBER & DATA SECURITY GUIDELINES FOR HEALTHCARE PROVIDERS

Endorsed by:

CSA SINGAPORE

INFOCOMM MEDIA DEVELOPMENT AUTHORITY

pdpc
PERSONAL DATA PROTECTION COMMISSION SINGAPORE

December 2023

Contents

1 Executive Summary

What is the Health Information Bill (HIB) about

1.1 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.

1.2 **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 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.

1.3 Entities under the scope of HIB include: i) Healthcare Services Act (HCSA) licensees; ii) Approved National Electronic Health Record (NEHR) users such as retail pharmacies; iii) MOH entities including MOH, MOH Office for Healthcare Transformation (MOHT), Health Promotion Board (HPB), Health Sciences Authority (HSA), MOH Holdings and its entities including Agency of Integrated Care (AIC) and ALPS, as well as National University Health System (NUHS), SingHealth, and National Healthcare Group (NHG); and iv) relevant community partners such as community care organisations.

Scope of the Cyber and Data Security Requirements under the HIB

1.4 As the HIB will require healthcare providers to meet cyber and data security requirements, MOH has developed the **Cyber and Data Security Guidelines for Healthcare Providers**, in consultation with the Cyber Security Agency of Singapore (CSA), Infocomm Media Development Authority (IMDA) and Personal Data Protection Commission (PDPC), to provide guidance on the measures to be put in place for the proper storage, access, use, and sharing of health information, in the lead up to the implementation of the HIB.

1.5 These Guidelines apply to healthcare providers with systems (e.g., desktops, laptops, servers, or devices) that either i) contain health information, or ii) connect with other systems containing health information. For avoidance of doubt, applicable data security requirements will apply to healthcare providers on pen-and-paper.

1.6 Standalone systems (i.e., not connected with other systems containing health information) that purely store non-health information (e.g., files containing only administrative information such as employee personal particulars or contact details) are excluded from the scope of the Guidelines.

1.7 Similarly, while the Guidelines do not prescribe specific obligations on healthcare providers' third-party vendors, products, or services (e.g., Clinical Management Systems (CMSes), cloud storage services), healthcare providers shall ensure that their choice of third-party vendors, products, or services is able to support them in meeting the security requirements under the Guidelines.

Summary of the Cyber and Data Security Requirements

1.8 The key cyber and data security aspects under the HIB are listed in **Table 1** below:

Table 1: Key Cyber & Data Security Aspects

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.
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 Security & Internal Audit Requirements • Regular checks on corporate policies and processes to ensure compliance and identify vulnerabilities.

Implementation of the Cyber & Data Security Requirements

1.9 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 HIB.

1.10 The requirements are expected to be imposed on the various healthcare providers in phases, considering: i) sectoral readiness and prevailing capabilities, ii) availability of implementation support plans to uplift cyber and data security posture in the sector, and iii) when mandatory data contribution to the NEHR will be enforced.

1.11 For further clarification or feedback on the Guidelines, healthcare providers may write to HIA_Enquiries@moh.gov.sg or go.gov.sg/cyber-data-guidelines-feedback.

2 Introduction

2.1 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.

2.2 To better safeguard patient safety and support care continuity, MOH will be introducing 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.

2.3 **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.; 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.

2.4 The HIB will require healthcare providers[1] to meet cyber and data security requirements in order to contribute and/or access to the NEHR safely.

2.5 In conjunction, the **Cyber and Data Security Guidelines for Healthcare Providers** (**"Guidelines"**) were developed in consultation with CSA, IMDA and PDPC[2], and build on the current set of Healthcare Cybersecurity Essentials (HCSE) 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, in the lead up to the implementation of the HIB.

2.6 The Guidelines also provide healthcare providers an early opportunity to understand the cyber and data security requirements needed to comply with the HIB, and to provide feedback to MOH where needed, on areas requiring greater clarity. The requirements are expected to be imposed on the various healthcare providers in phases, considering: i) sectoral readiness and prevailing capabilities, ii) availability of

[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, MOHT, 2 Statutory Boards (Health Promotion Board and Health Sciences Authority), MOH Holdings and its entities (AIC, ALPS) and the 3 public healthcare clusters (NUHS / SingHealth / NHG); and iv) relevant community partners (e.g., community care organisations).
[2] For avoidance of doubt, meeting the requirements within the Guidelines does not equate to compliance with the Personal Data Protection Act (PDPA).

implementation support plans to uplift cyber and data security posture in the sector, and iii) when mandatory data contribution to the NEHR will be enforced.

3 Objective and Scope

3.1 The healthcare sector remains among the top three targets[3] of cyber threats such as ransomware attacks, and it is critical that healthcare providers take steps to secure their IT assets and health information, and address vulnerabilities. Globally, cyber-attacks on healthcare organisations have impacted patient care, business continuity, and resulted in loss of confidential data. In August 2023, a major healthcare provider in the United States with a network of 17 hospitals and 166 outpatient clinics across various states suffered a ransomware attack[4] that led to a breach of an estimated 500,000 personal data from both employees and patients *(including social security numbers, medical profiles and histories, financial and legal information which have been offered for sale on the dark web)* and complete halt of its clinical operation services. In Singapore, ransomware and phishing continue to be persistent threats, with more than one ransomware case reported[5] to the CSA every three days and phishing attempts more than doubling over 2022. More ransomware-related resources, trends and possible decryption tools, can be found in the joint CSA-SPF Ransomware Portal.

3.2 Hence, the Guidelines 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.

3.3 These Guidelines apply to healthcare providers with systems (e.g., desktops, laptops, servers, or devices) that either i) contain health information, or ii) connect with other systems containing health information. For avoidance of doubt, applicable data security requirements will still apply to healthcare providers on pen-and-paper.

3.4 Standalone systems (i.e., not connected with other systems containing health information) that purely store non-health information which are not relevant to the provision of healthcare services to individuals (e.g., files containing only administrative information such as employee personal particulars or contact details) are excluded from the scope of the Guidelines.

3.5 Similarly, while the Guidelines do not prescribe specific obligations on healthcare providers' third-party vendors, products, or services (e.g., CMSes, cloud storage services), healthcare providers shall ensure that their choice of third-party vendors, products, or services is able to support them in meeting the security requirements under the Guidelines.

[3] CSA – Singapore Cyber Landscape 2022 – Top 3 Sectors targeted by Ransomware Attacks in 2022
[4] The Health Insurance Portability and Accountability Act (HIPAA) – Medical Records from Prospect Medical Holdings Ransomware Attack appear on Dark Web
[5] CSA – Singapore Cyber Landscape 2022 – Key Trends and Statistics of Malicious Cyber Activities observed in Singapore's Cyber Landscape in 2022

3.6 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 HIB.

4 How to use these Guidelines?

4.1 These Guidelines are structured into two sub-sections:

i. "*Why is this important?*", which explains the rationale and importance of the recommendations and provide examples to contextualise the recommendations to the healthcare environment; and

ii. "*What should healthcare providers do?*", which sets out concrete actions that healthcare providers can take to comply with the recommendations.

4.2 The key Cyber and Data Security aspects under the Guidelines (**Figure 1)** are summarised by the following acronyms:

i. **Cybersecurity**: **U**pdate software, **S**ecure endpoints, **B**ackup data, and **A**sset management ("**USB-A**").

ii. **Data Security**: **S**ecure sensitive data, **I**dentify and classify data assets, **A**ccess to data only for authorised users**.** ("**SIA**").

iii. **Common Cyber and Data Security Requirements**: **O**utsource safely and appropriately, **R**esponse to incident, **D**ispose assets securely, **E**mergency planning and contingency, **R**eview **S**ecurity ("**ORDERS**").

Figure 1: Key Cyber and Data Security Aspects under the Guidelines

Cybersecurity

Update – *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 – *Backup 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 types of data your organisation has, where they are stored, and secure them.

Data Security

Secure – *Storage, Reproduction, 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 Security 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 & Contingency Planning

- Supports ability to withstand service disruptions to ensure business continuity.

Review Security & Internal Audit

- Regular checks on corporate policies and processes to ensure compliance and identify vulnerabilities.

5 Cybersecurity

Update: Install software updates on your devices and systems promptly

Why is this important?

5.1 Manufacturers and developers of software release regular updates or patches, which not only add new features, but also fix security vulnerabilities that have been discovered. Any network connected system could be affected, including desktop and laptops; clinical, personnel or financial information systems; databases containing sensitive digital health information and images; mobile devices; and medical equipment. Using a system with outdated software also runs a higher risk of malware infection, which could also be passed to secondary users through exchange of emails or data.

5.2 Therefore, it is critical that users update their software regularly, failing which, attackers can take advantage of existing flaws to break into corporate networks, steal or encrypt data, gain control over a user's computer, or cause the malfunction of IT systems and medical devices.

What should healthcare providers do?

5.3 The healthcare provider shall prioritise the implementation of critical or important updates from established software companies or legitimate sources for operating systems and applications (e.g., security patches) to be applied as soon as possible. Updates shall be 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.

Secure/Protect – Use anti-malware and anti-virus solutions to protect against malicious software

Why is this important?

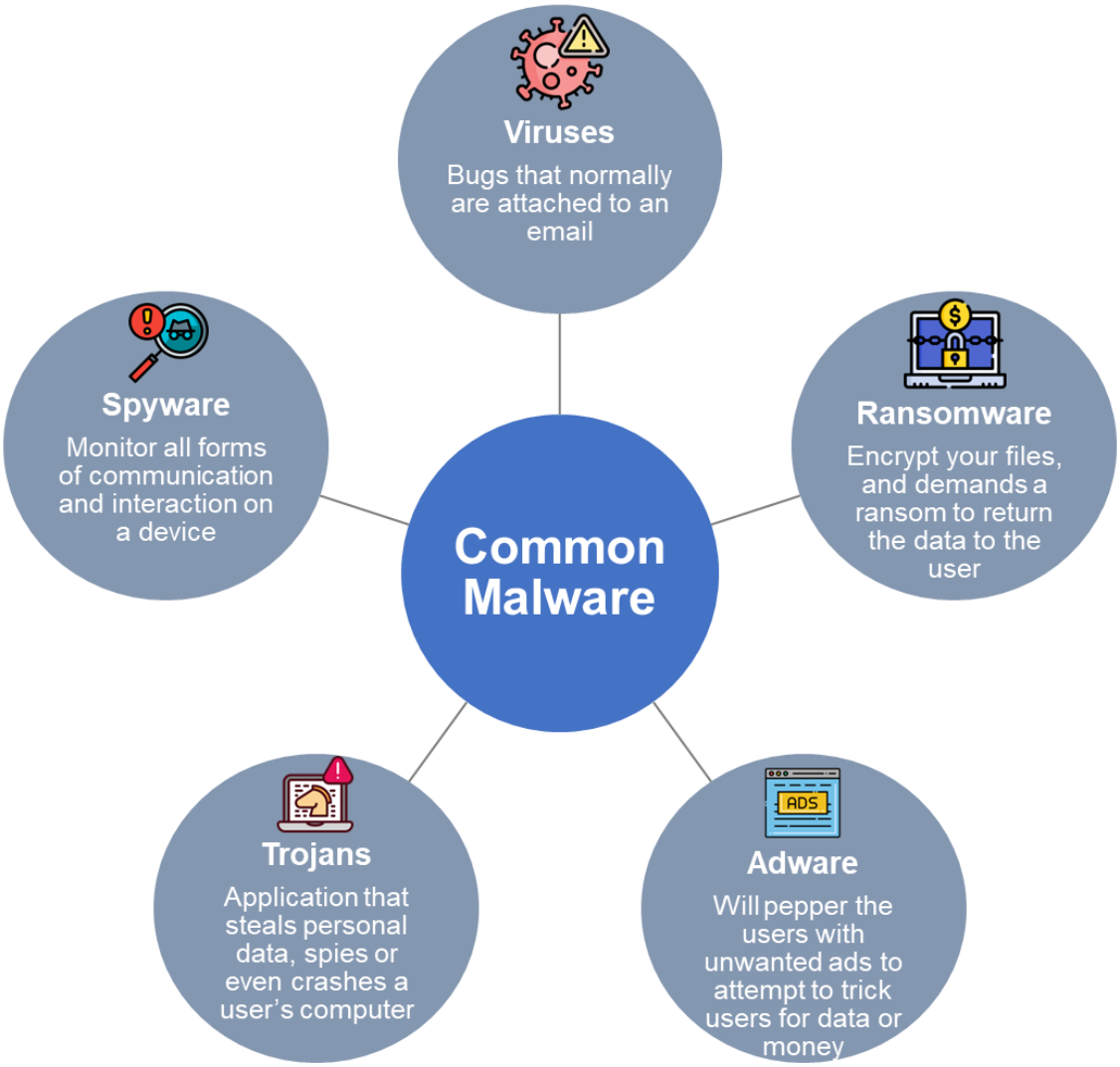
5.4 Just like a disease, malware (short for 'malicious software') is any programme or file that infects a software and causes harm to systems. Malware can find its way onto a computer in various ways (e.g., opening an infected email attachment, browsing a malicious website, or using a Universal Serial Bus (USB) memory stick that is carrying malware). Malware types (**Figure 2**) can include computer viruses, ransomware, adware, spyware, and trojans. Malware can perform a variety of functions such as stealing, encrypting, or deleting sensitive patient data, or hijacking core functions of machines such as causing medical devices to malfunction.

5.5 A particularly common type of malware in the healthcare sector is ransomware. Ransomware is used by cyber attackers to prevent access to important healthcare data or cause malfunction of systems such as clinical, personnel and financial information systems, databases containing health records, and medical devices – until the victim makes a payment to regain functionality of their computers or systems i.e., extortion. An attacker might also be able to read, modify, export (or steal), and even publicly release the affected digital health records and data. Paying of ransom to the attacker is strongly discouraged as it does not guarantee that the organisation will be granted the original functionality of its computers and systems. In fact, the ransomware can remain dormant and lead to further attacks in future.

5.6 Therefore, malware protection software is essential for proper protection against malware and cyberattacks. For instance, anti-malware solutions are installed to pre-emptively detect vulnerabilities in systems through regular scans and thereby isolating or removing software and files infected by malware. With numerous anti-malware solutions available in the market, organisations can consider the following factors when deciding the purchase of a solution:

i. Automatic update and scanning capabilities – given that malware and virus threats are constantly evolving;
ii. Malware removal capabilities – some solutions can only detect and quarantine malware at most (i.e., unable to remove malware);
iii. User-friendly features – easy navigation and adjustments of settings according to an organisation's needs;
iv. Cost-awareness – while most reputable security companies offer free versions of their anti-virus apps with basic protection, an organisation should consider paid versions with more comprehensive protection and features; and
v. Existing product reviews from reputable, trustworthy, and independent sources.

Figure 2: Common Types of Malwares



What should healthcare providers do?

5.7 Anti-malware solutions shall be used and installed in endpoints to detect attacks on the healthcare provider's environment. Examples of endpoints include laptops, desktops, and servers.

5.8 Virus and malware scans shall be carried out to detect possible attacks. Where feasible, scans should always be automated and remain active to provide constant protection.

5.9 Anti-malware solutions shall be configured to auto-update signature files or equivalent (e.g., non-signature-based machine learning solutions) to detect new malware. Where possible, signature updates should take place at least daily to stay protected from the latest malware.

5.10 Anti-malware solutions shall be configured to automatically scan the files upon access. This includes files and attachments downloaded from the Internet through the web browser or email, and external sources such as from portable USB drives.

5.11 Firewalls shall be deployed or switched on to protect the network, systems, and endpoints such as laptops, desktops, and servers.

5.12 A network perimeter firewall shall be configured to analyse and accept only authorised network traffic into the healthcare provider's network (e.g., a Local Area Network (LAN) made up of a group of computers or devices in the same physical location connected over a network). Examples could include packet filter[6], Domain Name System (DNS) firewall and application-level gateway firewall with rules to restrict and filter network traffic. Depending on the healthcare provider's network setup, the firewall functionality may be integrated with other networking devices, or as a standalone device.

5.13 The healthcare provider shall ensure its employees install or access only authorised software or attachments from official or trusted sources. This requirement may be met in different ways, e.g., install an application control solution that is integrated with antivirus software that uses both whitelisting and blacklisting to prevent unauthorised applications (including malware) from running. The whitelist takes reference from the list of organisation's authorised assets and review the list of blocked applications from the application control solution and remove all unnecessary applications.

5.14 The healthcare provider shall ensure employees use trusted network connections (e.g., mobile hotspot, personal Wi-Fi, corporate Wi-Fi, and Virtual Private Network (VPN)) for accessing the organisation's data or business email as opposed to the use of publicly available network connections. The healthcare provider shall also

[6] Packet filters are used in the process of passing or blocking data packets based on IP addresses, ports, or protocols.

educate employees of the risks of using publicly available network connections, which are highly accessible and vulnerable against cyber-attacks (e.g., spoofing attacks that set up fake access points to look like Wi-Fi connections for gaining access to a system or stealing information).

5.15 The healthcare provider shall ensure its employees are aware of the need to report any suspicious email or attachment to the IT team and / or senior management immediately.

Secure/Protect: Implement access control measures to control access to your data and services

Why is this important?

5.16 Most operating systems on computers provide two main types of user accounts:

i. **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.
ii. **User accounts** – These accounts are for users who need to run applications but do not need to perform any of the above functions.

5.17 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 activities such as entering clinical information into the Electronic Medical Record (EMR) and billing patients for consultation, administrative accounts are not required. Thus, ensuring that only authorised users are given the essential access rights to perform their work helps to reduce the risk of information being stolen, or hardware and software being compromised.

5.18 Passwords are an easy target for cyber-attackers. Multi-factor authentication (MFA) requires users to submit at least two factors (**Figure 3)** to prove their identity to gain access to a device or application. It is more difficult for an attacker to gain access to a device or application when multiple factors are required for authentication. If one factor is compromised, the attacker still has at least one more barrier to breach before successfully breaking into the target.

Figure 3: Common Factors for Multi-Factor Authentication (MFA)

What should healthcare providers do?

5.19 Healthcare providers shall have a system of account management to maintain and manage the inventory of accounts. This requirement may be met in different ways, e.g., using a spreadsheet, exporting the list from the software directory service.

5.20 The account inventory list shall contain minimally the following details, for the user, administrator, third-party, and service accounts:

i. Name;
ii. Username;
iii. Department;
iv. Role/Account Type;
v. Date of access created; and
vi. Last log-on date

5.21 The healthcare provider shall have a process to grant and revoke access only when the appropriate approvals are granted. This requirement may be implemented in different ways, e.g., email approval, or access request form. Approvals for any change in access to devices or applications shall be sought when there are personnel changes such as onboarding of new staff or change of role for employees. The following fields shall be captured for staff who are granted access to accounts:

i. Name;
ii. System to access;
iii. Department;
iv. Role/Account type;
v. From date; and
vi. To date

5.22 Access shall be managed to ensure that employees can access only the information and systems required for their job role.

5.23 Accounts with access rights that are no longer required, or have exceeded the requested date, shall have their access disabled, or removed from the system upon a periodic review[7] of the access rights of all accounts. Shared, duplicate, obsolete, and invalid accounts shall be removed *(frequency depends on a healthcare provider's operating needs and circumstances).* For example, this can include reviewing the privileges required for all accounts and give users, other than the administrator, the least user privileges necessary to carry out his / her work. Similar access rights reviews[8] shall be conducted for access to health information.

5.24 The administrator account shall only be accessed to perform administrator functions with approval from the senior management. Staff with administrator privileges should only use it when required, and regularly review user privileges according to the scope of the user in the institution.

5.25 Account password shall be changed in the event of any suspected compromise or lost tokens. Healthcare providers should also ensure that staff do not share passwords or tokens.

5.26 Healthcare providers shall ensure that all default passwords are replaced with a strong passphrase. A strong passphrase is usually at least 12 characters long and include upper case, lower case, and/or special characters. In setting passwords, publicly known information, or predictable character combinations (e.g., “password”, “qwerty” or “abc”) shall be avoided.

5.27 Healthcare providers shall not use the same password to encrypt all electronic storage mediums or computer devices (e.g., setting one password across the board for all accounts).

5.28 Healthcare providers shall ensure that each personnel is provided with unique user accounts (i.e., not to be shared) whenever possible.

5.29 User account shall be disabled and / or locked out after multiple failed login attempts, e.g., after 10 failed login attempts.

[7] Old, unused, or obsolete accounts and/accesses must be deleted from the system within 5 working days from completion of the review. If there is a need to retain the accounts (e.g., for tracing accountability, etc.), the access rights of these accounts must be deleted from the affected systems minimally.

[8] The review of access rights to health information shall be conducted under the following scenarios:

a) Staff resignation/retirement by the last day of service;
b) Termination of employment by the last day of service; and
c) Updating of user access rights based on a need-to-know basis shall be done within 14 business working days (e.g., change in staff's role, redeployment of staff).

5.30 Access shall be managed to ensure third-parties / contractors can access only the information and systems required for their job role. Such access shall be removed once they no longer require them.

5.31 Two-factor authentication (2FA) shall be used for administrative access (including remote access) to important systems, such as an Internet-facing system containing sensitive or business-critical data. This requirement may be implemented in different ways, e.g., use of an authenticator application on the mobile or one-time password (OTP) token.

5.32 Third-party or contractors working with sensitive information in the organisation shall sign a Non-Disclosure Agreement (NDA) form. The form should include the consequences (e.g. damages) for failure to abide by the agreement.

5.33 Physical access control shall be implemented to allow only authorised employees or contractors to access the healthcare provider's IT assets and/or environment, e.g., use of cable lock to lock the workstations and card access door lock to authenticate and authorise entry.

5.34 The healthcare provider shall maintain log-in rules (i.e., tracking of users logging[9] in and out of systems) properly and review them periodically, and ensure that only authorised individuals have access to security logs.

Secure/Protect: Secure Configuration – Use secure settings for your organisation's procured hardware & software

Why is this important?

5.35 Secure configuration refers to security measures that are implemented when developing and installing computers and network devices to reduce unnecessary cyber vulnerabilities. Hardware and software first procured from manufacturers usually come with default settings typically geared towards initial ease of deployment and use. For example, in the case of a router, this could be a predefined password, or for an operating system, it could be the standard applications that come installed. Hardware and software are not secure in their default settings, and vulnerabilities could be easily exploited by threat actors to compromise systems and gain unauthorised access to data.

5.36 Healthcare providers should adopt sufficient protection measures to secure the configurations of their hardware and software in order to reduce the risk of attacks that

[9] Security and audit logs serve as records of who have accessed the IT network or systems and what operations they have performed. Having such logs is useful to establish baseline, identify suspicious trends, and critical for understanding the nature of security incidents (i.e., during an active investigation and postmortem analysis). If it is impossible to enable logging on all systems or devices, healthcare providers should also keep a manual log.

take advantage of well-known default administrator settings, passwords, exploits, or vulnerabilities.

What should healthcare providers do?

5.37 Security configurations shall be implemented for assets, including desktops, servers, and routers. This requirement may be met in different ways, e.g., choosing systems with MFA functionality to manage and access patient and corporate information, adopting industry recommendations and standards such as the Centre of Internet Security (CIS) benchmarks on configuration guidelines across multiple vendor products, and running security baseline analyser and system configuration scripts.

5.38 Weak or default configurations shall be avoided or updated before assets are used, e.g., changing default password and performing a deep scan with an anti-malware solution instead of using a standard scan.

5.39 Insecure configurations and weak protocols shall be replaced or upgraded to address the associated vulnerabilities, e.g., using Hypertext Transfer Protocol Secure (HTTPS) over normal HTTP to encrypt data communication and upgrading Wired Equivalent Privacy (WEP) to Wi-Fi Protected Access 2/3 (WPA2/WPA3) to enhance the Wi-Fi security standards.

5.40 Features, services, or applications that are not in used shall be disabled or removed, e.g., disabling file sharing service, software macros, internet connection, remote admin access, and File Transfer Protocol ports.

5.41 Automatic connection to open networks and auto-run feature of non-essential programs (other than backup or anti-malware solution, etc.) shall be disabled.

Back up: Back up essential data and store them offline

Why is this important?

5.42 A backup is a copy of the files on a computer which is stored separately (either offline or offsite). Hardware failure, theft, or malware infection (especially ransomware) can make recovering critical data expensive or impossible. Furthermore, failure to back up critical data can also jeopardise patient safety. Conversely, having a recent backup of the data will aid the healthcare provider in recovering from a cyber-attack or data breach more quickly with lesser resources required.

What should healthcare providers do?

5.43 The healthcare provider shall identify business-critical systems and those containing essential business information and perform backup. What needs to be backed up is guided by identifying what is needed for business recovery and continuity in the event of a cybersecurity incident. Examples of business-critical systems for healthcare providers include CMSes and EMRs.

5.44 The backups shall be performed on a regular basis, with the backup frequency aligned to the business requirements and how many days' worth of data they can afford to lose.

5.45 If the scope includes cloud environment, the healthcare provider shall:

i. Understand the role and responsibility between itself and the cloud service provider in terms of data backup, e.g., cloud shared responsibility model, scope, and coverage of the cloud service; and
ii. Ensure there are alternative forms of data backup being utilised to ensure business continuity, e.g., storing the backups in a hard disk drive, purchasing the backup services by the cloud service provider, and adopting multiple clouds as backups.

5.46 All backups shall be protected from unauthorised access and be restricted to authorised personnel only. Backups should minimally be password-protected.

5.47 Backups shall be stored separately (i.e., offline) from the operating environment. Where feasible, backups should be stored offsite, e.g., a separate physical location.

5.48 Longer term backups such as monthly backups shall be stored offline in an external secure storage location, e.g., password-protected USB flash drives, encrypted external hard disks and/or tape storage at an alternative office location.

5.49 Backups shall be tested annually, or more frequently, to ensure that business-critical systems and essential business information can be restored effectively.

Asset: People – equip staff with cyber-hygiene practices as the first line of defence

Why is this important?

5.50 Cyberattacks often exploit human weaknesses to gain unauthorised access to an organisation's IT system. These commonly happen in the form of phishing, where attackers disguise themselves as legitimate individuals or reputable organisations via email instant messaging or other communication channels to fraudulently obtain personal details and user credentials to gain access to networks, distribute trojan malware in the systems, launch ransomware attacks, or insider threats. In extreme cases, cyberattacks can disrupt the healthcare organisation's ability to provide care and other life-saving capabilities when the organisation's access to critical patient information is locked by the cyber-attackers.

5.51 Employees are often the first line of defence in the organisation, and also the weakest link in the security chain since they are vulnerable to social engineering attacks (e.g., using false promises or threats to entice a victim to reveal system access passwords, before stealing personal information or infecting computer systems with malwares). Users may not follow security practices for several reasons, such as a lack of knowledge, perceived inconvenience from having to meet security measures, or forgetfulness. Therefore, developing a good cyber hygiene culture amongst employees can strengthen organisational defence against cyberattacks. For any successful information security programme, addressing and mitigating the impact of bad human behaviour and practices is critical.

What should healthcare providers do?

5.52 Healthcare providers shall ensure employees attend cybersecurity awareness training periodically so that they are aware of the security practices and behaviour expected of them. This requirement may be met in different ways, e.g., through regular internal training of staff on the healthcare provider's cyber and data security policies and practices, employees going through self-learning cybersecurity resource materials, engaging external training providers, or conducting simulated phishing exercises for staff.

5.53 Cyber hygiene practices and guidelines shall be developed for employees to adopt in their daily operations, to ensure that they are aware of the security practices and behaviours expected of them. For example, the cyber hygiene practices and guidelines should include the following topics to mitigate incidents arising from the human factor. **Table 2** lists examples of measures that can be considered for developing cyber hygiene practices and guidelines:

i. Protect yourself from phishing;
ii. Set strong passphrase as passwords;

iii. Protect your corporate and/or personal devices (used for work);
iv. Report cyber incidents;
v. Handle and disclose business-critical[10] data carefully; and
vi. Work onsite and remotely in a secure manner

5.54 For more information, please refer to CSA's Cybersecurity Toolkit for Employees).

Table 2: Examples of Measures for Cyber Hygiene Practices & Guidelines

Topic	Examples of Measures
Protect yourself against phishing	• Spot signs of suspected phishing email (e.g., urgent call to action or threats, spelling errors, bad grammar, suspicious links, or unexpected attachments). • Never click any links or attachments in a suspected phishing email. • Report the phishing email and delete it.
Set strong passphrase as passwords	• Use strong passphrase with at least twelve characters long with upper case, lower case, and / or special characters. • Keep the passphrase unpredictable (e.g., avoid using publicly available information such as family last name or birthday). • Avoid using the same password for multiple accounts.
Protect your corporate and/or personal devices (used for work)	• Always know where your devices are and never leave them unattended. • Secure your device with digital keys such as passphrases, Personal Identification Numbers (PINs), or biometric locks. • Ensure that your devices have the necessary security settings enabled and regularly back up your device's data in an external storage device or online storage service.
Report cyber incidents	• Spot signs of cyber incidents (e.g., failure to access organisation's files, slowness of web browsers, unknown files appearing). • Report the incident immediately to your IT or security teams to investigate further. • Refrain from taking action on your own as it may alert the cyber attackers that their activity has been spotted.
Handle and disclose business-critical data carefully	• Be aware of and adhere to the organisation's data management policy (e.g., policies to identify and manage confidential and / or sensitive data, risk classification of confidential and / or sensitive data). • Ensure the recipient of the confidential and / or sensitive data is authorised to access the data. • If you suspect any unauthorised or accidental disclosure of confidential and / or sensitive data, immediately inform the recipient to delete the confidential and / or sensitive data.
Work onsite and remotely in a secure manner	• Adhere to clear desk and clear screen policy (e.g., lock documents with confidential and/or sensitive data in the cabinet and not leave them unattended). • Connect to a Virtual Private Network (VPN) when accessing your organisation's resources remotely. If VPN is not available, connect to secured networks such as personal Wi-Fi hotspot secured with a passphrase.

[10] Business-critical data refers to any type of data in a healthcare provider's possession or control that is vital and confidential to its operations, including clinical / health data, administrative data (e.g., patients' personal data) and / or other important non-health data (e.g., financial information).

Asset: Hardware & Software – Identify the hardware and software used in your organisation, and protect them

Why is this important?

5.55 An up-to-date inventory of all IT hardware[11] and software[12] assets enable healthcare providers to identify what they need to protect and detect unauthorised hardware or software in their network. If healthcare providers are unaware of the hardware and software assets being used, they run the risk of not knowing the security vulnerabilities and risks their assets which are exposed to. To limit unnecessary exposure to unknown security risks, it is also important for healthcare providers to only deploy hardware and software which are essential or critical for its operations.

What should healthcare providers do?

5.56 Healthcare providers shall maintain an up-to-date inventory of assets used in the organisation for:

i. All hardware (e.g., medical devices, Personal Computer (PCs), laptops, printers, modems, and network routers); and
ii. All software (e.g., CMSes, EMRs, accounting, and Human Resource (HR) software, Microsoft Word and Excel, medical devices with network connectivity, and third-party[13] software or tools).

5.57 This requirement may be met in different ways e.g., use of spreadsheet or a IT asset management software. **Table 3** provides guidance on the minimum details that should be included in the asset inventory list for hardware and software assets.

[11] End-user devices (e.g., desktops, laptops, medical devices as well as portable and mobile devices such as tablets and mobile phones), network devices such as firewalls and routers, non-standard computing devices such as Internet of Things (IoT) devices and servers (e.g., email, web, and application servers).
[12] Software includes business applications, online accounts for which business email addresses are used, and other applications accessed either locally or remotely via the devices.
[13] Third-party software and devices refer to those which are not developed in-house or may have been purchased off-the-shelf and used by healthcare providers.

Table 3: Minimum Details to be included for Hardware & Software Asset Inventory Lists

Hardware Asset	Software Asset
Hardware name/model	Software name
Asset tag[14]/serial number	Software publisher
Asset type	Software version
Asset location	Business purpose
Network address	Asset classification
Asset owner	Approval/Authorised date
Asset classification[15]	End-of-Support (EOS) date
Department	
Approval/Authorised date	
End of Support (EOS) date	

5.58 The healthcare provider shall develop a protocol to authorise new hardware and software into the organisation. This requirement may be met in different ways including, e.g., obtain email approval from the senior management, ensure that new hardware and software are procured from official or trusted sources, ensure that the cybersecurity capability of the medical devices commensurate with the risk of the environment that it is deployed in (e.g., via the upcoming voluntary CSA Cybersecurity Labelling Scheme for Medical Devices), perform malware scans to verify that the asset is clean, and maintain an asset whitelist / blacklist.

5.59 The date of authorisation of any software and hardware shall be keyed into the asset inventory list after obtaining the relevant approvals, e.g., obtain an email approval, or via an approval form from the relevant authority within the organisation. Software and hardware without an approval date shall be removed.

5.60 Software shall only be installed if needed on corporate devices[16]. Any devices shall be disconnected and software to be uninstalled from the corporate IT network when they are no longer in use. Only corporate devices shall be used when accessing patient and corporate information.

5.61 Hardware and software assets that are unauthorised or have reached the End-of-Support (EOS) shall be replaced. End-of-Support (EOS) refers to the point when a company ceases technical servicing for a product e.g., limited tech support, software updates, or repairs.

5.62 In the event of any continued use of EOS assets, the healthcare provider shall assess the risk, obtain approval from the senior management, and monitor its use until the asset is replaced.

[14] Asset tag should provide unique identification for each of the asset, e.g., it can be concatenated with acronyms of the asset type, department pre-fix and a running number to form a unique identifier.
[15] Asset classification involves identifying the value of each asset in an organisation and prioritising security measures to protect these assets and ensure their confidentiality, integrity, and availability.
[16] Depending on the business needs of the healthcare provider, non-corporate devices may be used if these are installed with Mobile Device Management (MDM) (or equivalent solutions) with full cybersecurity controls, e.g., 2FA, remote wipe, having data residing in cloud storage instead of devices, etc.

Asset: Data – Identify the types of data your organisation has, where they are stored, and secure them

Why is this important?

5.63 The confidentiality, integrity, and availability of patient's health information is integral in enabling healthcare professionals to deliver accurate and appropriate care and uphold patient safety. As healthcare providers digitalise and rely on technology to enhance their day-to-day operations, it is also important to put in place measures to secure business-critical data in endpoints (e.g., personal data within EMRs) to safeguard patient's health information.

What should healthcare providers do?

5.64 The healthcare provider shall establish policies and processes to identify and protect its business-critical data. The policies may include classification of business-critical data in terms of its sensitivity, and impact on patient safety, care continuity and critical operations, with appropriate measures, such as password-protection, encryption of personal data (at rest) and/or emails, to secure the data at rest and in transit where applicable *(for more information, please refer to data security classification section).*

5.65 The policies and processes shall also include measures to prevent employees from leaking confidential and / or sensitive data outside of the organisation. This requirement may be met in different ways e.g., controlled access, disabling USB ports.

6 Data Security

Note: *All data security requirements under the "What should healthcare providers do?" sub-sections are applicable to both electronic data (e.g., data residing in systems) and non-electronic (e.g., data displayed in hardcopy document) data, and where appropriate, are illustrated with examples for clarity.*

Secure: Storage Requirements – Store your health information securely to prevent unauthorised access

Why is this important?

6.1 Data storage requirements are intended to protect the data storage resources and the data stored – both on-premises and in external data centres as well as the cloud – from accidental or deliberate damage or destruction, and from unauthorised users and uses. Secure storage of data assures the confidentiality, integrity, and availability of the data to support the organisation's operations.

6.2 If the health information is not securely stored, it will be difficult to detect and trace the source of data leakage as the personnel in possession of the information is no longer limited to only the authorised users. Therefore, having robust data storage measures protect organisations against the risks of data theft, data tampering, accidental data corruption or destruction.

What should healthcare providers do?

6.3 Healthcare providers shall define retention periods for Sensitive Normal / Sensitive High health information in accordance with any applicable legislation (e.g., PDPA, MOH-related requirements), contractual requirements (e.g., funding agreement, data sharing agreement), and/or national standards or guidelines.

6.4 Healthcare providers shall ensure that Sensitive Normal / Sensitive High health information is secured from unauthorised access or loss, as follows:

i. Within the office premises, Sensitive Normal / Sensitive High health information shall be protected against unauthorised access by other parties e.g., hardcopy documents are stored in access-controlled locations within the office or under lock and key, laptops or portable storage media devices containing sensitive data are locked up when not in use.
ii. Where healthcare providers use commercial storage facilities, healthcare providers shall ensure the following:
    a. The facility services procured meet the security requirements (i.e., healthcare providers had conducted due diligence checks on their credibility, reviewed their security policies to assess for appropriate security controls on the stored data);
    b. Maintain proper records to indicate materials containing sensitive data deposited in offsite storage; and

c. Conduct audits to ensure materials are intact or in order and have not been subject to unauthorised access.

Secure: Reproduction Requirements – Do not reproduce copies of sensitive health information unless necessary

Why is this important?

6.5 Reproduction of data involves the process of copying and storing data in multiple locations to improve data availability and accessibility i.e., a key component of data resilience and disaster recovery strategies. Hence, organisations benefit from a reliable access to an accurate and up-to-date copy of data during unexpected system failures, or data breaches.

6.6 However, the existence of multiple copies of health information in an organisation also increases the possibility of the information being exposed to unauthorised access or loss if not safeguarded properly. When necessary, organisations are advised to only make copies of health information for approved work purposes or to carry out specified job functions.

What should healthcare providers do?

6.7 Copies of Sensitive Normal / Sensitive High health information shall only be made by authorised parties on a need-to-know basis and where relevant to the purpose of use, and according to any established corporate policies.

6.8 When making copies of Sensitive Normal / Sensitive High health information using external devices or at external locations, healthcare providers shall ensure that they maintain possession of any copies of the Sensitive Normal / Sensitive High health information (e.g., when staff of a healthcare provider makes photocopies of health records outside of the office premises, the staff must not leave the photocopied materials unattended at the photocopier).

Secure: Conveyance Requirements – Transport health information properly to avoid unwanted data exposure

Why is this important?

6.9 Conveyance of health information (e.g., when staff brings sensitive materials from one clinic to another clinic) may increase the risk of unauthorised users gaining access to the health information.

6.10 The healthcare provider shall set parameters on when a health information can be conveyed out of its premises, and when to implement security controls to provide adequate protection during conveyance.

What should healthcare providers do?

6.11 If healthcare providers must transfer any Sensitive Normal / Sensitive High health information in public or transmit health information electronically, the healthcare provider shall ensure that:

i. Its personnel do not carry health information to locations for non-work purposes;
ii. The materials are kept in its personnel's possession / control at all times;
iii. The health information is prevented from accidental exposure (e.g., where another person can see the information in plain sight); and
iv. When transmitting health information electronically, e.g., by email, the files are password-protected and are sent to the right recipients[17].

For more information, please refer to the PDPC guides on Data Protection Management Programme and Data Protection Impact Assessment.

Identify: Data Security Classification – Know the information sensitivity levels of the data to apply appropriate safeguards

Why is this important?

6.12 Data security classification provides visibility into the data types and corresponding workflows in an organisation to protect data (i.e., where data is processed, stored, and how they are accessed). By categorising data according to sensitivity, healthcare providers can understand its value, determine the associated risks, and establish clear boundaries around handling and protecting the data. In dynamic environments, particularly when data resides in the cloud, on-premises or shared with external services, data security classification also provides a systematic approach towards the protection of sensitive health information.

6.13 Properly classifying health information according to its sensitivity levels can allow healthcare providers to implement the appropriate security safeguards for protection against unauthorised access. It also allows healthcare providers to take a targeted approach towards data security, invest strategically in protection measures where the risk is the greatest, and identify or dispose of unnecessary data. In addition, categorised data also enables security teams to spot vulnerabilities quickly, and fix issues that compromise sensitive data.

[17] Password-protection or encryption of health information is mandatory if there is at least 1 individual's health information classified as Sensitive High, or 500 or more individuals' health information classified as Sensitive Normal.

What should healthcare providers do?

6.14 The healthcare provider shall have policies and / or processes in place to ensure that it has a good understanding of all health information that resides in its organisation. This allows the healthcare provider to apply the appropriate data security classification (i.e., Sensitive Normal or Sensitive High as highlighted in **Table 4**) and implement the corresponding safeguards to all of the healthcare information in its possession or under its control. For avoidance of doubt, health information *(as defined in the Introduction section)* in the context of HIB will be minimally classified as Sensitive Normal.

For more information, please refer to PDPC's Guides on Data Protection Management Programme and Data Protection Impact Assessment.

Table 4: Data Classification and Examples of Data Types

Data Classification	Examples of Data Types[18]
Non-Sensitive	• Anonymised Data (i.e., cannot be associated with specific individuals.)
Sensitive Normal	• General Health Information • Medical/Lab Reports • Discharge Summaries • Genomic Information (excluding Whole Genome and/or Whole Exome Sequences) • Demographics Information, e.g., race, ethnicity
Sensitive High	• Sensitive Health Information (e.g., HIV, mental disorders such as schizophrenia, delusional disorders, substance abuse and addictions). <*Please refer to the MOH corporate website for the full list.*>

6.15 Where health records contain health information tagged with a combination of information security classification (e.g., both Sensitive Normal and Sensitive High in the same record), the security safeguards of the higher classification shall be applied to the record.

6.16 As prevailing data security classifications of health information may change over time, the healthcare provider shall conduct appropriate assessments to review if existing data classifications remain appropriate and in line with MOH's policy, including any timely re-classification of health information where relevant.

[18] The list of data types provided are examples of health information that fall under Sensitive Normal and Sensitive High and is non-exhaustive.

6.17 Depending on its operating context, the healthcare provider shall consider using appropriate tools to document the healthcare information in its possession or under its control, such as developing a data inventory map or data flow diagram/chart that captures information like:

i. **Type and description of data** e.g., clinical assessment forms, patient referral forms, patient medical records;
ii. **Sensitivity classification of data** e.g., Sensitive Normal or Sensitive High based on the highest classification imposed;
iii. **Medium the data resides as** e.g., hardcopy records, electronic records;
iv. **Storage of data** e.g., hardcopy records in cabinets or offsite Data Centres and electronic records in online / cloud storage services or storage devices such as thumb drives;
v. **Retention period** e.g., each type of health information should have a specific retention period according to the purpose of retention such as due to business purpose, to comply with a legal obligation; and
vi. **Disposal method** e.g., for healthcare information that had been disposed at the end of the retention period, what the mode of disposal was (e.g., paper shredded according to DIN 66399 standards[19], in-house disposal facility or engage third-party vendors to dispose of healthcare information), when the date of disposal was, who the staff in charge of disposal were.

Identify: Marking Requirements – Differentiate data of varying information sensitivity levels by marking their classification

Why is this important?

6.18 As different pieces of health information may have different information sensitivity classifications, marking allows users to correctly identify the information sensitivity tagged to the health information that they are handling, and understand the impact and potential consequences of losing the health information.

6.19 Marking may apply to:

i. Data residing on physical data storage assets (e.g., a physical label that is visible to users who handle the physical data); and
ii. Documents residing in a folder / directory in an electronic system (e.g., inserting sensitivity classification in the footer, header, or watermark of internal documents containing health information).

What should healthcare providers do?

6.20 The healthcare provider shall have policies in place for the marking[20] of Sensitive Normal / Sensitive High health information to enable its staff to recognise

[19] Please refer to PDPC Guide on Disposal of Personal Data on Physical Medium for more information.
[20] Suggested considerations for marking include the following:

the sensitivity of data they are handling, such as an organisation-wide policy requiring all documents containing health information to be manually or electronically labelled as Sensitive Normal / Sensitive High, as the case may be. In situations where a healthcare provider has assessed that it is impractical to mark all the documents and data as all the data it handles is classified, the healthcare provider shall reflect clearly within its corporate policy that "all data within the organisation is classified as Sensitive Normal / Sensitive High" in place of marking the individual documents and their staff should comply with the corresponding security requirements.

Access: Authorised Users – Restrict access to health information for valid and relevant purposes

Why is this important?

6.21 To minimise the incidence of misuse or accidental data leakages, all health information shall only be made accessible to authorised users. When health information is extensively shared within a healthcare provider, there is an increased risk of inadvertent exposure to unauthorised users, which can occur through the following:

i. Intentional and inappropriate disclosure of health records; or
ii. Loss or theft of belongings containing health records.

What should healthcare providers do?

6.22 Access to any Sensitive Normal or Sensitive High health information shall only be granted to staff who have fulfilled all the following conditions:

i. **Need-to-Know**: Staff[21] that have legitimate need to access the individual's Sensitive Normal / Sensitive High health information to carry out their work functions as determined by an appropriate authority within the healthcare provider (e.g., a clinician is granted access rights to the healthcare provider's EMR so he can access a patient's healthcare record to understand the patient's medical condition(s) and carry out appropriate patient care).

a) Types of classified materials (e.g., Sensitive Normal or Sensitive High).
b) Formats of classified materials (e.g., physical document, electronic format).
c) Party / user that is handling the classified material (e.g., staff of healthcare provider that handles such data on day-to-day basis and is relatively familiar with the associated security classification, a third-party vendor managing or delivering classified materials on behalf of the healthcare provider).
d) Intent of the security marking (e.g., to inform third-party vendor of the classified materials it is handling and protect the materials accordingly).
e) Practicality of security marking (e.g., cost of IT system enhancements, manual stamping of hard copy materials).

[21] Staff includes any third-parties that Sensitive Normal or Sensitive High health information have been shared with.

ii. **Data Security-Briefed**: Staff have been informed or made aware of and acknowledged[22] the data protection and security requirements in these Guidelines and prevailing laws e.g., PDPA, and / or healthcare provider's corporate policies.

[22] Examples of acknowledgement include sending an email on data security with email recipients responding "I understand the data security requirements" or records of attendance to briefing sessions.

7 Common Requirements for Cyber & Data Aspects

Outsourcing & Vendor Management: Understand the responsibilities set between your organisation and vendor

Why is this important?

7.1 Third-party software, hardware and services are commonly procured off-the-shelf and used by healthcare providers as they do not typically design or develop them in-house. Having a clear understanding of the roles and responsibilities between healthcare providers and third-party vendors, and the safeguards that will be put in place for third-party products or services helps an organisation to secure its systems against potential threats.

What should healthcare providers do?

7.2 If healthcare providers are using an IT service provider to manage their network, systems, and medical devices, they shall:

i. Clearly understand the services and security practices that the IT service provider will provide; and
ii. 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.

7.3 When using third-party software and devices, healthcare providers shall:

i. Ensure that they clearly understand:

   a) How patient and corporate data is processed, transferred, and stored;
   b) The safeguards that vendors have in place to secure the third-party software and devices they provide, including any assurance on activities carried out (e.g., CSA Cyber Essentials certification for CMS vendors, audits);
   c) What the contractual arrangements with vendors are, including responsibilities of each contractual party in the event of an incident or breach; and

ii. Subscribe to security-related alerts published by vendors for the third-party software and devices their practice uses.

7.4 If healthcare providers are using cloud services (e.g., Amazon Web Services, Google Drive), they shall ensure that the division of responsibilities for setting security configurations is clearly defined and understood.

7.5 Where healthcare providers store their Sensitive Normal or Sensitive High health information online and / or procure third-party products or services (e.g., online storage facilities, cloud service providers) to do so, the healthcare providers shall assess any known risks associated with using such services (such as researching on the credibility and reliability of the third-party vendors, enquiring on scope of service such as how data is processed, transferred, and stored, assessing appropriate legal instrument to apportion accountability or risks, etc.) and to refrain from using any vendors found to be unsafe.

For more information, please refer to the Chapter on Cloud Services in PDPC's Advisory Guidelines on Selected Topics (Chapter on Cloud Services).

Incident Response: Prepared to detect, respond, and recover from incidents

Why is this important?

7.6 Cyber incidents and data breaches can have a huge impact on a healthcare provider's reputation, financial stability, productivity, and patient's confidence and trust in the organisation's ability to safeguard personal health information. For example, a data breach (whether is it a result of a cyber-attack or human error) occurs when health information held by healthcare providers is lost or subjected to unauthorised access. This can happen under various scenarios, such as:

i. Unauthorised access to systems containing health information;
ii. Inappropriate disclosure of health information by staff; or
iii. Loss or theft of laptops, mobile devices, removable storage devices, or paper records containing health information.

7.7 A cyber / data incident response plan allows the healthcare provider to mitigate the impact of an incident quickly and uphold patient confidentiality and trust.

What should healthcare providers do?

7.8 The healthcare provider shall establish an up-to-date basic incident response plan to guide the organisation on how to respond, manage and mitigate the impact of cyber or data incidents (such as those involving Sensitive Normal / Sensitive High health information). Examples include, e.g., phishing, ransomware, and data breach. The plan shall contain the following details:

i. Clear roles and responsibilities of key personnel in the healthcare provider involved in the incident response process;
ii. Procedures to detect, respond, and recover from the common cyber / data threat scenarios, e.g., phishing, ransomware, data breach; and

iii. Communication plan and timeline to escalate and report the incident to internal and external stakeholders (such as regulators, customers, and senior management).

7.9 The incident response plan shall be made aware to all employees in the organisation that have access to the organisation's IT assets and/or environment. All staff should also be aware of how to report suspicious activity and possible incidents based on the obligations under prevailing legislative or regulatory requirements.

7.10 More information on the key components and steps in an incident response plan, please refer to CSA's resource on Incident Response Checklist.

Disposal Requirements: Proper disposal of health information mitigates the risk of unauthorised access

Why is this important?

7.11 When health information is improperly disposed of, there is a risk that unauthorised users may gain access without the healthcare provider's knowledge and result in undesired data exposure. Proper disposal of the health information involves destroying data stored on a device or medium such that recovery and access by unauthorised users is impossible. This is important for protecting the privacy and confidentiality of health information after it is no longer required or used.

What should healthcare providers do?

7.12 Before disposing any hardware asset or data, healthcare providers shall ensure that there is secure destruction (e.g., shredding physically stored data, encrypting hard disk before reformatting, and overwriting electronic data in a storage medium completely) of Sensitive Normal / Sensitive High health information (e.g., after the determined data retention period expires or when there is no business or legal use for the health information).

Emergency Planning for Contingency: Supports ability to withstand service disruptions to ensure business continuity

Why is this important?

7.13 In the healthcare sector, service disruptions can affect day-to-day healthcare operations and potentially impact patients' care, especially when time-sensitive medical interventions are involved. An organisation's ability to maintain critical operations in the event of unanticipated events and emergencies (e.g., natural disasters, cyber-attacks, or human negligence resulting in data leak) is vital for business continuity and disaster recovery – i.e., developing the appropriate

capabilities, plans and testing to prepare organisations and their employees to be able to withstand disruptions.

What should healthcare providers do?

7.14 The healthcare provider shall:

i. Establish a business continuity plan to ensure organisational resilience (e.g., identifying critical assets that require high availability and putting in place redundancies) against the common business disruption scenarios including those caused by cyber incidents and data breaches, and execute it when needed.
ii. Regularly review the relevance and test the effectiveness of the organisation's business continuity plan through planned scenario-based training or exercises.

Review Security & Internal Audit Requirements: Regular checks on corporate policies and processes to ensure compliance and identify vulnerabilities

Why is this important?

7.15 Regular security reviews and internal audits are important as they help organisations identify potential vulnerabilities (e.g., outdated software security patches, inadequate password policies, unrestricted staff access to patient health information, etc.), and take corrective actions to prevent any cyber / data incident. This also ensures that all employees working for a healthcare provider are aware of the need to comply with the implemented security safeguards in an organisation, prevailing cyber / data security legislation, as well as any security policies that have been established by the healthcare provider.

What should healthcare providers do?

7.16 Healthcare providers shall review their compliance with implemented cybersecurity and data security safeguards for Sensitive Normal / Sensitive High health information. This requires the provider to conduct checks (e.g., self-assessment audits conducted internally or by external auditors) to review established corporate policies, staff compliance with measures in place, as well as intervene timely in the event of a lapse in compliance (e.g., rectifying the lapses, conduct further training for staff on SOPs to prevent similar occurrences and strengthen security measures where necessary).

*<**Note:** The proposed incident reporting thresholds and timelines for cyber or data incidents under the HIB are summarised in **Table 5** and are subject to further review prior to the actual implementation of the HIB requirements. Specific details of how healthcare providers can report the incidents to MOH will be shared when available.>*

Table 5: Proposed Incident Reporting Thresholds & Timelines under the HIB

	Cybersecurity Incidents	**Data Breaches**
Reporting Thresholds	• A notifiable [23] cybersecurity incident involves: i. a computer or computer system containing health information or interconnected with a computer or computer system containing health information; and ii. The computer or computer systems are under the healthcare provider's control.	• Aligned to PDPA's data breach notification threshold. • In the context of health information, a notifiable data breach is one that: i. results in, or is likely to result in, significant harm to an affected individual (i.e., breach contains sensitive health information); or ii. is, or is likely to be, of a significant scale (i.e., impact on equal or more than 500 affected individuals).
Reporting Requirements	• Initial notification to MOH within 2 hours after healthcare provider assesses that the incident is a notifiable cybersecurity incident or data breach meeting the reporting thresholds. • Affected healthcare provider to provide an incident report within 14 days of initial notification. • Healthcare provider must notify affected individuals at the same time, or as soon as practicable after notifying MOH, if the incident causes, or is likely to cause significant harm to an individual.	

8 Clarifications & Feedback

8.1 For further clarification or feedback on the Guidelines, healthcare providers may wish to submit their responses via HIA_Enquiries@moh.gov.sg or go.gov.sg/cyber-data-guidelines-feedback.

[23] Notifiable cybersecurity incidents include but are not limited to e.g., unauthorised hacking of computer or computer systems, installation or execution of unauthorised software or computer codes of malicious nature, attempts to prevent the availability of computer information or services to its intended users (i.e., denial of service attacks), attempts to intercept the traffic between two computer or computer systems to steal or alter information (i.e., man-in-the-middle attack), etc.

9 Appendix

Note: *This checklist provides a quick overview of the security requirements and should be read in-conjunction with the "Cyber & Data Security Guidelines for Healthcare Providers."*

Cyber and Data Security Checklist

A. Cybersecurity	YES	NO	Remarks
[A1] Update: Install software updates on your devices and systems promptly			
[A1.1] We have a process to implement critical or important software updates (e.g., security patches) released for all our IT applications as soon as possible.			
[A2] Secure/Protect: Use anti-malware and anti-virus solutions to protect against malicious software			
[A2.1] All our IT end points (e.g., laptops, desktops, and servers) have anti-malware solutions installed to detect cyber-attacks on our systems (e.g., performing regular virus and malware scans).			
[A2.2] Our anti-malware solutions are configured to automatically scan files (e.g., attachments downloaded from the Internet, and external sources such as from portable USB drives) upon access.			
[A2.3] We have deployed firewalls to protect the network, systems, and endpoints.			
[A2.4] Our firewalls are configured to analyse and accept only authorised network traffic into our network.			
[A2.5] Our organisation's cyber hygiene policies and practices include all of the following: • Only authorised software or attachments from official or trusted sources shall be installed. • Use trusted network connections (e.g., corporate Wi-Fi, and Virtual Private Network (VPN)) when accessing the organisation's data or business email. • All suspicious email or attachment are reported to the IT team and / or senior management immediately.			
[A3] Secure/Protect: Implement access control measures to control access to your data and services			
[A3.1] We have a system and inventory to maintain and manage access accounts where employees can access only the information and systems required for their job role.			
[A3.2] We have a process to regularly review user privileges and the inventory of access accounts to ensure the following:			

• Accounts are disabled or removed when access rights are no longer required or have exceeded the requested date. • Shared, duplicate, obsolete, and invalid accounts are removed in a timely manner. • Access to administrator accounts are approved by the senior management.			
[A3.3] We have policies and procedures in place to ensure the following: • Each staff has their own access accounts, passwords, and tokens i.e., no sharing of accounts, passwords, and tokens amongst staff. • Account passwords are changed in the event of any suspected compromise or lost tokens. • All default passwords are replaced by a strong passphrase when systems or devices are deployed for use in the organisation.			
[A3.4] Use different passwords to encrypt all electronic storage mediums or computer devices (e.g., setting one password across the board for all accounts).			
[A3.5] Our organisation has a policy of disabling and / or locking user accounts after multiple failed login attempts, e.g., after 10 failed login attempts.			
[A3.6] Third-parties or contractors working with sensitive information have signed a Non-Disclosure Agreement (NDA) form.			
[A3.7] We have physical access controls to authenticate and authorise employees or contractors' access to our organisation's IT assets e.g., use of cable lock to lock the workstations and card access door lock.			
[A3.8] Maintain log-in rules (i.e., tracking of users logging in and out of systems) properly and review them periodically, and ensure that only authorised individuals have access to security logs.			
[A4] Secure/Protect: Secure Configuration – Use secure settings for your organisation's procured hardware & software			
[A4.1] Our organisation's security configurations for hardware and software include all of the following policies and practices: • Update weak, insecure or default configurations on assets before using them. • Remove or disable features, services, or applications that are not in used. • Disable automatic connection to open networks and auto-run feature of non-essential programs (other than backup or anti-malware solution, etc.).			

[A5] Back up: Back up essential data and store them offline			
[A5.1] Our organisation's policies for backing up data includes all of the following policies and practices: • Backing up identified business-critical systems and those containing essential business information. • Perform backups on a regular basis. • Protect all backups from unauthorised access (minimally password-protected) and restrict backups to authorised personnel only. • Store backups separately (i.e., offline) from the operating environment, and where feasible, stored offsite, e.g., a separate physical location. • Store longer term (e.g., monthly) backups offline in an external secure storage location. • Test backups at least annually to ensure that business-critical systems and essential business information can be restored effectively.			
[A5.2] Where cloud services are used to back up data: • My organisation understands the roles and responsibilities between itself and the cloud service provider in terms of data backup. • My organisation ensures that we also have alternative forms of backing up of data e.g., storing the backups in a hard disk drive, purchasing the backup services by the cloud service provider, or adopting multiple clouds as backups.			
[A6] Asset: People – equip staff with cyber-hygiene practices as the first line of defence			
[A6.1] Our employees attend cybersecurity awareness training at least once a year.			
[A6.2] Our employees adopt cyber hygiene practices and guidelines in their daily operations and are aware of the security practices and behaviours expected of them.			
[A7] Asset: Hardware & Software – Identify the hardware and software used in your organisation, and protect them			
[A7.1] Our organisation's policies and practices for managing assets include all of the following: • Maintain an up-to-date asset inventory of hardware and software used in the organisation. • Have a protocol to authorise new hardware and software into the organisation. • Include the date of authorisation of any software and hardware in the asset inventory list. • Install software only if needed on the corporate devices; disconnect and uninstall any devices or software from the corporate IT network respectively when they are no longer in use. • Replace any hardware and software assets that are unauthorised or have reached End-of-Support (EOS).			

[A8] Asset: Data – Identify the types of data your organisation has, where they are stored, and secure them			
[A8.1] Our organisation establishes policies and processes to identify and protect its business-critical data, including measures preventing employees from leaking confidential and / or sensitive data.			

B. Data Security	YES	NO	Remarks
[B1] Secure: Storage Requirements – Store your health information securely to prevent unauthorised access			
[B1.1] We define retention periods for Sensitive Normal / Sensitive High health information in accordance with any applicable legislation (e.g., PDPA, MOH-related requirements), contractual requirements (e.g., funding agreement, data sharing agreement), and/or national standards or guidelines.			
[B1.2] Our organisation secures Sensitive Normal / Sensitive High health information from unauthorised access or loss, whether they are stored within the office premises or in commercial storage facilities.			
[B2] Secure: Reproduction Requirements – Do not reproduce copies of sensitive health information unless necessary			
[B2.1] We have policies and procedures in place to: • Specify the circumstances, purposes, and authorised parties for copies of Sensitive Normal / Sensitive High health information to be made. • Ensure that copies of Sensitive Normal / Sensitive High health information are made only by authorised parties. • Maintain possession of any copies of Sensitive Normal / Sensitive High health information when these are transported and / or used in external locations. *Example*: When staff of a healthcare provider makes photocopies of health records outside of the office premises, the staff must not leave the photocopied materials unattended at the photocopier.			
[B3] Secure: Conveyance Requirements – Transport health information properly to avoid unwanted data exposure			
[B3.1] When we transfer any Sensitive Normal / Sensitive High health information in public or transmit health information electronically, we ensure that: • Staff do not carry health information to locations for non-work purposes. • The materials are kept in the staff's possession / control at all times. • The health information is prevented from accidental exposure (e.g., where another person can see the information in plain sight). • When transmitting health information electronically, e.g., by email, the files are password-protected and are sent to the right recipients.			
[B4] Identify: Data Security Classification – Know the information sensitivity levels of the data to apply appropriate safeguards			
[B4.1] All health information in our possession or under our control is appropriately classified as Sensitive Normal or Sensitive High.			

[B4.2] We review if existing data classifications remain appropriate and in line with MOH's policy, including any timely re-classification of health information where relevant.			
[B4.3] All our documents containing health information are manually or electronically labelled as Sensitive Normal / Sensitive so that staff recognise the sensitivity of the data they are handling. If it is impractical to mark all the documents and data as all the data handled is sensitive, the corporate policy should clearly state that "all data within the organisation is classified as Sensitive Normal / Sensitive High" in place of marking the individual documents and ensure that all staff comply with the corresponding security requirements.			
[B5] Access: Authorised Users – Restrict access to health information for valid and relevant purposes			
[B5.1] We grant access to any Sensitive Normal or Sensitive High health information only to staff on a need-to-know basis and those who are aware of the relevant data protection and security requirements.			

C. Common Cyber & Data Security Requirements	YES	NO	Remarks
[C1] Outsourcing & Vendor Management: Understand the responsibilities set between your organisation and vendor			
[C1.1] When a vendor is engaged to manage our network, systems, and medical devices, we are clear of the services and security practices that the IT vendor provides; and are updated regularly by the IT vendor on vulnerability reports and updates about security issues for the systems they are managing on our behalf.			

[C1.2] When using third-party software and devices, we:
 	
• Clearly understand:
  ○ How patient and corporate data is processed, transferred, and stored;
  ○ The safeguards that vendors have in place to secure the third-party software and devices they provide, including any assurance on activities carried out (e.g., CSA Cyber Essentials certification for CMS vendors, audits);
  ○ What the contractual arrangements with vendors are, including responsibilities of each contractual party in the event of a cybersecurity or data incident or breach; and
 	
• Subscribe to security-related alerts published by vendors for the third-party software and devices in use.			

[C1.3] When we use cloud services, we clearly define and understand the division of responsibilities between our organisation and the cloud service provider, for setting security configurations.			
[C1.4] When we store Sensitive Normal or Sensitive High health information online and / or procure third-party products or services (e.g., online storage facilities, cloud service providers) to do so, we assess any known risks associated with using such services and do not use any vendors found to be unsafe.			
[C2] Incident Response: Prepared to detect, respond, and recover from incidents			
[C2.1] Our organisation has an up-to-date incident response plan to guide us on how to respond, manage, and mitigate the impact of cyber or data incidents. The incident response plan includes: • Clear roles and responsibilities of key personnel in our organisation involved in the incident response process; • Procedures to detect, respond, and recover from the common cyber / data threat scenarios, e.g., phishing, ransomware, data breach; and • Communication plan and timeline to escalate and report the incident to internal and external stakeholders (such as regulators, customers, and senior management).			

[C2.2] All employees in our organisation that have access to the organisation's IT assets and / or environment are aware of: • The incident response plan. • All staff are aware on how to report suspicious activity and possible incidents based on the obligations under prevailing legislative or regulatory requirements.			
[C3] Disposal Requirements: Proper disposal of health information mitigates the risk of unauthorised access			
[C3.1] We destroy all Sensitive Normal / Sensitive High health information that we no longer require or use before disposing any hardware asset of data.			
[C4] Emergency Planning for Contingency: Supports ability to withstand service disruptions to ensure business continuity			
[C4.1] Our organisation has a business continuity plan to ensure organisational resilience (e.g., identifying critical assets that require high availability and putting in place redundancies) against the common business disruption scenarios including those caused by cyber incidents and data breaches, and execute it when needed.			
[C4.2] We regularly review the relevance and test the effectiveness of the organisation's business continuity plan through planned scenario-based training or exercises.			
[C5] Review Security & Internal Audit Requirements: Regular checks on corporate policies and processes to ensure compliance and identify vulnerabilities			
[C5.1] Our organisation conducts internal audits on compliance with the implemented cyber and data security safeguards for Sensitive Normal / Sensitive High health information; and implements appropriate corrective and preventive measures where non-compliances are identified.			