# HEALTH INFORMATION BILL: CYBER & DATA SECURITY GUIDEBOOK FOR HEALTHCARE PROVIDERS

## VERSION 1.4

## APRIL 2025

**DEVELOPED BY AIC AND MOH**

# Contents

# Introduction

With an increase in the contribution, access and sharing of health information across the ecosystem, this puts our healthcare system at increasing risk of cyber-attacks. Coupled with the consequences of potential data breaches and losses, it is critical for healthcare providers to ensure measures are in place to protect and safeguard health information. As custodians of patients' healthcare data, healthcare providers contributing to or accessing NEHR, or participating in data sharing use cases enabled under the upcoming Health Information Bill (HIB) will have to meet a set of cyber and data security requirements to protect both electronic and non-electronic health information.  The HIB will establish the framework to govern the safe collection, access, use, and sharing of health information across the healthcare ecosystem, to facilitate better continuity and seamless transition of care.

The contents of the HIB Cyber and Data Security Guidebook are intended to assist healthcare providers in comprehending the requirements of the HIB "Cyber and Data Security Guidelines for Healthcare Providers" that were published by MOH in December 2023. The guidebook was developed by referencing existing Personal Data Protection Commission and Cyber Security Agency resources. All references and links cited in the guidebook are accurate as of the publication date. This resource provides explanations, practical examples, and templates/resources (where applicable) to address specific requirements. The guidance in this guidebook should not be construed as the only and definitive way to meeting the HIB Cyber and Data Security requirements. Healthcare providers are ultimately responsible for the policies, processes and practices in protecting health information under their care.

The HIB Cyber and Data Security Guidelines and this guidebook are available on the HIB website and AIC Partners Page:

- https://www.healthinfo.gov.sg
- https://www.aic.sg/partners/

# How to Use This Guide

<u>Interpretation of the Columns in this Document</u>

| Column A | Column B | Column C |
|---|---|---|
| • [Reference Number] Refers to the Health Information Bill Cyber and Data Security requirements that were published in December 2023 | • Explanation of the Health Information Bill Cyber and Data Security requirements in column A by providing guidance and examples, that are meant to be non-exhaustive, of how the requirements can be met [Note: "Shall" is used to indicate a mandatory requirement while "Should" is used to indicate a recommendation.] | • Refers to resources / templates to provide further guidance to meet column A requirements |

# 1. Cyber Security

| S/N | (A)<br>MOH HIB requirements | Guidelines for HIB Guidebook | | |
| --- | --- | --- | --- | --- |
| | | (B)<br>Explanation on MOH HIB Requirements | | (C)<br>Help and Resources |
| | **[1] Updates: Install software updates on your devices promptly** | | | |
| 1 | 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. | **1.** The organisation shall develop a policy to prioritise the implementation of critical software updates and patches.<br><br>*Examples of legitimate sources for security updates:*<br><br>***Official websites**.*<br>*Most software companies maintain official websites where users can download updates directly. For instance, Microsoft provides security updates for Windows operating systems through its official website.*<br><br>***Security advisories.***<br>*Some legitimate sources provide security advisories or bulletins detailing vulnerabilities and patches. These advisories often come directly from software vendors, SingCERT (The Singapore Cyber Emergency Response Team, under CSA), or other trusted organizations.*<br><br>**2.** The policy shall be reviewed and updated periodically to align with the evolving cyber threat landscape.<br><br>**3.** The policy shall include a patch cycle with the following:<br><br>**a) Categorization**<br>Categorization of updates and patches based on the risk and impact to the business and operations, e.g., Critical, High, Medium and Low.<br><br>**b) Implementation timeline**<br>A timeline corresponding with the appropriate patch category defined above in a) shall be defined. | | Organisations may refer to the following resources:<br><br>1. NIST: Guide to Enterprise Patch Management Planning<br>https://doi.org/10.6028/NIST.SP.800-40r4<br><br>2. Sample patch management standard<br><br>PDF<br><br>Patch-Management-Standard.docx_safe.pdf |

| S/N | (A)<br>MOH HIB requirements | Guidelines for HIB Guidebook | | |
|---|---|---|---|---|
| | | (B)<br>Explanation on MOH HIB Requirements | | (C)<br>Help and Resources |
| | | *Example:*<br>*Critical: Within 3 working days*<br>*Low: Within 8 weeks*<br><br>*Note: Organisation should review their operational and risk consideration before determining the frequency and practical timeline prior to documentation in the patch policy.* | | |
| 2 | 5.3 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. | **1.** When determining the patch timeline in the patch policy, Organization shall take into consideration, systems that are critical to patient care.<br><br>For systems that are linked to patient care, due consideration should be taken during the patching cycle so that patient safety is not impacted.<br><br>**2.** Organisation shall validate the update / patching of the system with software vendors and compatibility testing should be conducted prior to deployment.<br><br>**3.** Automatic updates for critical operating systems and application patches shall be enabled where feasible to receive the latest updates.<br><br>Applicable for the below services:<br>**a) Mobile devices such as mobile phone, tablet, etc.** | | Cloud Security for Organisations (csa.gov.sg)<br><br>https://www.csa.gov.sg/our-programmes/support-for-enterprises/sg-cyber-safe-programme/cloud-security |

| S/N | (A)<br>MOH HIB requirements | Guidelines for HIB Guidebook | |
|---|---|---|---|
| | | (B)<br>Explanation on MOH HIB Requirements | (C)<br>Help and Resources |
| | | The organization shall ensure that updates and patches for mobile devices are only downloaded from trusted sources (i.e., official app store from the manufacturer).<br><br>**b) IoT devices**<br>The organization shall remove or replace any IoT devices (e.g., CCTV, printers) that are not receiving any software patches or updates.<br><br>**c) Cloud**<br>The organization shall refer to the cloud shared responsibility model with its Cloud Service Provider (CSP). This will give clarity to the organization on when they are responsible for software updates and security patches, and when the CSP is responsible.<br><br>The organization shall have visibility on the software updates and security patches done by its CSPs.<br><br>The organization shall also have security requirements regarding software updates defined for its CSPs. | |
| | **[2] Secure and Protect: Use anti-malware and anti-virus solutions to protect against malicious software** | | |
| 3 | 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. | **1.** The organisation shall implement an anti-malware solution and the solution should be centrally managed.<br>To ensure support for the anti-malware solution, Commercial-off-the-shelf (COTS) solutions shall be used and continually subscribed in order to get update and patches.<br><br>**2.** The organisation should consider implementing advanced anti-malware solutions such as Endpoint Detection and Response (EDR) and Advanced Threat Protection solutions for a more adequate and enhanced protection.<br><br>Such protection should cover services or solution such as FTP, email and any downloads to end user computing device, servers and | |

| S/N | (A)<br>MOH HIB requirements | Guidelines for HIB Guidebook | | |
|-----|------------------------------|----------------------------------|----|----|
| | | (B)<br>Explanation on MOH HIB Requirements | (C)<br>Help and Resources | |
| | | personal devices that interact with provider(s) system or network. This should include OT or IoT devices/network.<br><br>**3.** The anti-malware solution shall be installed at all endpoints (including but not limited to personal computers, servers BYOD and IoT) to protect the devices from viruses and malware. | |
| 4 | 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. | **1.** The anti-malware solution shall be configured to:<br><br>**a)** be in an active state;<br><br>**b)** conduct scheduled scans of the system; | |
| 5 | 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. | **c)** ensure live definition updates are automatically turned on;<br><br>**d)** prevent users from changing the configuration and turning off or uninstalling the solution.<br><br>**e)** active scanning shall be turned on to protect files and attachments from services or solutions such as but not limited to FTP, email ~~to~~ or any downloads to the endpoints including OT or IoT devices/network. | |
| 6 | 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. | **2.** When determining the frequency and timing of the scheduled scan, the organisation should consider the impact of the scanning on system resources and to schedule the timing of the scans accordingly. Where possible, signature updates should take place at least daily to stay continue protected from the latest malware.<br><br>**3.** The organisation shall review the anti-malware report regularly to follow-up | |
| 7 | 5.11 Firewalls shall be deployed or switched on to protect the network, systems, and endpoints such as laptops, desktops, and servers | The organization shall protect their network with firewalls, including for devices such as but not limited to endpoints, personal computers, servers and BYOD.<br><br>Firewalls include: | |

| S/N | (A)<br>MOH HIB requirements | Guidelines for HIB Guidebook | |
|---|---|---|---|
| | | (B)<br>Explanation on MOH HIB Requirements | (C)<br>Help and Resources |
| | | **a)** Network firewall<br>For protecting the network from unauthorised network traffic.<br>*Example: F5 or Cisco firewall*<br><br>**b)** Host based firewall<br>For protection of operating systems for endpoints and servers, etc.<br><br>*Example: Microsoft Defender or Symantec Endpoint Protection* | |
| 8 | 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 filter6, 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. | **1.** Firewalls shall be configured to only allow legitimate traffic to be transmitted. Firewall rules such as "Any to Any" shall be disallowed.<br><br>**2.** The firewall rules shall be:<br><br>**a)** reviewed on a periodic basis such as at minimally half yearly.<br><br>**b)** removed when no longer required.<br><br>**c)** clearly documented and approved by appropriate management personnel. | |
| 9 | 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 | **1.** An authorised software list shall be established for software that is allowed installation onto a corporate device.<br><br>**2.** An authorisation process to review software for onboarding should be established.<br><br>**3.** Use of freeware or third-party software that are not approved by management should hence not allowed to be installed. | |

| S/N | (A)<br>MOH HIB requirements | Guidelines for HIB Guidebook | | |
|---|---|---|---|---|
| | | (B)<br>Explanation on MOH HIB Requirements | | (C)<br>Help and Resources |

| S/N | (A)<br>MOH HIB requirements | (B)<br>Explanation on MOH HIB Requirements | (C)<br>Help and Resources |
|---|---|---|---|
| | reference from the list of healthcare provider's authorised assets and review the list of blocked applications from the application control solution and remove all unnecessary applications. | Only authorised software or attachments from official or trusted sources shall be installed or accessed.  "Official or trusted sources" refer to reputable and reliable channels from which software or attachments can be obtained or accessed safely.<br><br>*Examples include:*<br><br>***Official Websites***<br>*The primary website of the software developer or vendor, where users can download software or attachments directly. These websites often have mechanisms to verify the authenticity of the software and provide support to users.*<br><br>***App Stores***<br>*Platforms like Apple's App Store, Google Play Store, or Microsoft Store are considered official sources for downloading software applications for their respective operating systems. These platforms vet applications for security and quality before making them available to users.*<br><br>**4.** Organisation shall conduct a check annually at minimum or at a frequency determined by Management to ensure compliance and licensing requirements are met. | |
| 10 | 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 healthcare provider's data or business email as opposed to the use of publicly available network connections.<br><br>The healthcare provider shall also educate employees of the risks of using publicly available network connections, which are highly accessible and vulnerable against | Trusted network refers to the users when using the network are aware of the provider of the network and assurance has been obtained that it is safe for use.<br><br>**1.** A Virtual Private Network (VPN) shall be implemented to ensure a trusted network connection for any remote access.<br><br>**2.** For employees who connect via BYOD to access corporate network remotely, such devices shall correspondingly be installed with a Mobile Device Management (MDM) solution to ensure trusted connection. | CSA website on Cybersecurity Toolkits (details of trusted network):<br>https://www.csa.gov.sg/our-programmes/support-for-enterprises/sg-cyber-safe-programme/cybersecurity-toolkits |

| S/N | (A)<br>MOH HIB requirements | Guidelines for HIB Guidebook | |
|---|---|---|---|
| | | (B)<br>Explanation on MOH HIB Requirements | (C)<br>Help and Resources |
| | 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). | There shall be containerization⁺ of corporate data and the ability to disable the extraction of data through copying or screen-capture of the data by the BYOD owner.<br><br>⁺Containerization refers to the process of segregating personal and corporate data on personal devices by creating a logical container/separate space to enhance corporate data security.<br><br>**3.** Organisation shall include policy requirements, best practices such as danger of using public wireless network as part of Cyber Security awareness and new employee on-boarding process and educate employees on the risks of using untrusted networks. | |
| 11 | 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. | Organisation shall communicate and make available the workflow on the immediate reporting of suspicious email/activities to its IT team or senior management.<br><br>*Example:*<br>*The organisation could establish an IT security mailbox or incident hotline for staff to report suspicious IT activities.* | |
| | **[3] Secure and Protect: Implement access control measures to control access to your data and services** | | |
| 12 | 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. | Organisation shall maintain an inventory listing of all access accounts either via a system or using spreadsheets.<br><br>*Note: When using a spreadsheet, organisation needs to ensure secure storage and protection of the spreadsheet from tampering and unauthorized access.* | Sample Account Management / Access Control Policy<br><br>📄 PDF<br><br>Account-Management-Access-Control-Stan |
| 13 | 5.20 The account inventory list shall contain minimally the following details, for the user, administrator, third-party, and service accounts: | **1.** The account inventory list shall be reviewed on a regular basis such as half yearly or annually and when there are changes in the | |

| S/N | (A)<br>MOH HIB requirements | Guidelines for HIB Guidebook | |
|---|---|---|---|
| | | (B)<br>Explanation on MOH HIB Requirements | (C)<br>Help and Resources |
| | i.     Name;<br>ii.    Username;<br>iii.   Department;<br>iv.   Role/Account Type;<br>v.    Date of access created; and<br>vi.   Last log-on date | organisational structure to prevent the misuse of the account and account privileges.<br><br>The frequency of the review shall be assessed based on operational requirements and risk and shall be approved by management and documented.<br><br>**2.** The account inventory list shall be updated whenever there is a change in:<br><br>**a)** staff movement such as new joiner, leaver or a change in department or job roles<br><br>**b)** systems or applications such as new systems or system decommissioning<br><br>**c)** access rights or roles for the account | |
| 14 | 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:<br><br>i.     Name;<br>ii.    System to access;<br>iii.   Department; | **1.** The organisation shall establish a process to review all accounts and account privileges on a regular basis such as at a minimum half yearly basis.<br><br>**2.** The review process shall include the following:<br><br>**a)** verification of the need to maintain the account and/or access rights with the assigned access rights reviewer (such as Reporting Officer, Head of Department or Management)<br><br>**b)** verify inactive users and accounts and/or access rights<br><br>**3.** Access control practices shall include:<br>a) approvals for any new accounts<br><br>**b)** Disable accounts when user is away | Sample Access Control Policy:<br><br>📄 PDF<br>Access-Control-Polic y.docx_safe (1).pdf |

| S/N | (A)<br>MOH HIB requirements | Guidelines for HIB Guidebook | | 
|---|---|---|---|
| | | (B)<br>Explanation on MOH HIB Requirements | (C)<br>Help and Resources |
| | iv.     Role/Account type;<br>v.     From date; and<br>vi.     To date | **c)** Revoke inactive accounts or access rights immediately<br><br>*An inactive ID refers to a prolong period where the account is not use or no transaction continuously up to X days as agreed by Management (example of X=90 days). Organisation should review the operational requirement and risk prior to defining the review period or X and this shall be documented.* | |
| 15 | 5.22 Access shall be managed to ensure that employees can access only the information and systems required for their job role. | **1.** Organisation shall maintain a user access matrix (UAM), documenting the access rights of the individual and applications. | Sample Roles & Permission Matrix:<br><br>https://i.dell.com/sites/doccontent/app-merchandizing/esupport/flatcontent/global/en/Documents/RoleDetails.pdf |
| 16 | 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 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 shall be conducted for access to health information. | **1.** Organisations shall grant user access based on the principle of least privilege where users or systems are granted the minimum rights and authorizations that they require to perform their functions.<br><br>**2.** Organisation shall establish a process to record user access requests and approvals and monitor such requests to ensure accounts and access rights are correctly granted.<br><br>**3.** User access reviews shall be conducted regularly, and accounts / access rights are removed if:<br>**a)** no longer required<br>**b)** exceeded requested date<br>**c)** if is a shared account<br>**d)** is a duplicate account<br>**e)** is obsolete<br>**f)** is invalid | |

| S/N | (A)<br>MOH HIB requirements | Guidelines for HIB Guidebook | |
| --- | --- | --- | --- |
| | | (B)<br>Explanation on MOH HIB Requirements | (C)<br>Help and Resources |
| 17 | 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. | **1.** Organisation shall establish a governance process to manage the use of administrative accounts.<br><br>**2.** Usage of administrative accounts shall require appropriate approvals by senior management prior to usage.<br><br>**3.** Each usage is required to be logged (e.g., via email or logbook), maintained and reviewed on a regular basis, such as at minimum quarterly.<br><br>**4.** Any unusual activities shall be investigated and reported to senior management. | |
| 18 | 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. | Organisation shall put in place procedures to ensure that passwords of accounts suspected to have compromised is to be changed immediately.<br><br>*Example:*<br>*Inform user with compromised account to change password immediately or enforced change password upon next logon at system level* | |
| 19 | 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. | **1.** Organisation shall replace all system account default passwords with a new password immediately before system goes live.<br><br>**2.** Organisation shall use passphrase as the default password configuration.<br><br>*Example of a passphrase: Ilov3myCurry@westside*<br><br>*Guidelines for creating strong password/passphrase:*<br><br>*a) Password minimum length should be 12 character long and shall include 3 of the 4 below combination: ~~of~~ upper cap, lower cap, number or special characters.* | |

| S/N | (A)<br>MOH HIB requirements | Guidelines for HIB Guidebook | | |
|---|---|---|---|---|
| | | (B)<br>Explanation on MOH HIB Requirements | | (C)<br>Help and Resources |
| 20 | 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). | **1.** Organisation shall ensure that the password policy includes the requirement that the same password shall not be used across multiple accounts.<br><br>**2.** The password policy shall clearly state that the same password for accessing systems should not be used for encryption purposes. Different passwords shall be set for each encryption use.<br><br>*Example: use of a password generator to manage and generate secure passwords/passphrases.* | | Sample Password Policy Guide from CIS:<br><br>https://learn.cisecurity.org/cis-password-policy-guide-passphrases-monitoring-and-more |
| 21 | 5.28 Healthcare providers shall ensure that each personnel is provided with unique user accounts (i.e., not to be shared) whenever possible | **1.** To ensure accountability and traceability, organisation shall disallow the sharing of accounts by employees.<br><br>**2.** Should a shared account be required; organisation shall establish clear and robust processes to ensure that any changes made can be traced and accounted to the individual that has made the changes. | | |
| 22 | 5.29 User account shall be disabled and / or locked out after multiple failed login attempts, e.g., after 10 failed login attempts. | **1.** To prevent password brute force attacks, user account lockout thresholds shall be configured to lockout after a defined number of failed login attempts.<br><br>**2.** The defined threshold shall be determined with support from business and operation teams to minimize the impact to operations while balancing security risks.<br><br>**3.** The defined threshold shall be endorsed by senior management.<br><br>*Example:*<br>*Defined threshold = 10 failed login attempts* | | |
| 23 | 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 | **1.** Organisation shall establish a clear access control matrix (UAM) where access rights shall be determined using role-based access rights for all staff and/or third-parties.<br>*Examples of third-parties:*<br>- *Vendors* | | |

| S/N | (A)<br>MOH HIB requirements | Guidelines for HIB Guidebook | |
|---|---|---|---|
| | | (B)<br>Explanation on MOH HIB Requirements | (C)<br>Help and Resources |
| | | - *Contractors*<br>- *Interns*<br>- *Part timers*<br><br>**2.** Organisation shall conduct user access reviews of the UAM on a regular basis, such as half yearly. | |
| 24 | 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 | **1.** Organisation shall put in place a matrix to determine system classifications according to the impact and significance of the system in nature.<br><br>**2.** Access to systems that are deemed critical to business operations and/or contain sensitive data shall be enforced with 2-factor authentication.<br><br>*Example of 2FA includes authentication program Microsoft Authenticator on mobile device or One time password (OTP).*<br><br>*Note: A system classification matrix should take into consideration the impact to the organisation based on the following:*<br>*Data sensitivity*<br>*Internet facing*<br>*System that has impact to patient record and patient care* | Information Security Classification Framework:<br><br>Information security classification framework (QGISCF) \| For government \| Queensland Government |
| 25 | 5.32 Third-party or contractors working with sensitive information in the healthcare provider shall sign a Non-Disclosure Agreement (NDA) form. The form should include the consequences (e.g. damages) for failure to abide by the agreement | **1.** Before commencing any sharing of information (i.e., health information, personal data or organisational sensitive data), a Non-Disclosure Agreement (NDA) shall be signed.<br><br>**2.** The NDA shall include penalties and consequences for non-compliances.<br><br>**3.** Organisation shall ensure that the coverage of the NDA and Service Level Agreement (SLA) includes adequate protections for the organisation. | Sample NDA:<br><br>📄 PDF<br>Example-One-Way-N<br>on-Disclosure-Agreen |
| 26 | 5.33 Physical access control shall be implemented to allow only authorised | **1.** Physical access to offices and IT systems or assets shall be restricted to only authorized personnel. | |

| S/N | (A)<br>MOH HIB requirements | Guidelines for HIB Guidebook | |
|---|---|---|---|
| | | (B)<br>Explanation on MOH HIB Requirements | (C)<br>Help and Resources |
| | 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. | Vendors that are authorized should be escorted when accessing IT assets and system.<br><br>**2.** All IT assets such as servers or network switches shall be physically secured . Example:  server racks.<br><br>**3.** Endpoint devices shall be secured physically. Example, secured with cable locks.<br><br>*Example of physical access controls are:*<br>*a) card access system*<br>*b) bio-metric access.* | |
| 27 | 5.34 The healthcare provider shall 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. | **1.** Organisation shall turn on audit trails and security logging to track user activities for systems and applications and review periodically to flag out possible inappropriate accesses.<br><br>**2.**For organisations that do not have a client / server environment, administrators need to ensure endpoint device logging are turned on.<br><br>**3.** Only administrators shall have access to the log file.<br><br>**4.** Log files shall be available upon request *(i.e., for incident investigations or upon request by regulators)* | |
| | **[4] Secure and Protect: Secure Configuration – Use secure settings for your organisation's procured hardware and software** | | |
| 28 | 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 | **1.** Organisation shall establish a baseline hardening standard.<br><br>*Example, from Centre of Internet Security (CIS), Cloud Security Alliance best practices etc.*<br><br>**2.** To enhance the security of systems from the exploitation of vulnerabilities by threat actors, organisation shall review industry standards and consider implementing the standards after taking operational needs into consideration. | Sample Configuration Management Policy from NIST:<br><br>PDF<br><br>Configuration-Manag ement-Policy.docx_saf |

| S/N | (A) MOH HIB requirements | Guidelines for HIB Guidebook | |
|---|---|---|---|
| | | (B) Explanation on MOH HIB Requirements | (C) Help and Resources |
| | on configuration guidelines across multiple vendor products, and running security baseline analyser and system configuration scripts. | | Sample Secure Configuration Standard:<br><br>📄 PDF<br><br>Secure-Configuration -Standard.docx_safe.p<br><br>Cloud Security Guidance from Cloud Security Alliance:<br><br>📄 PDF<br><br>csa_security_guidanc e_v4.0.pdf_safe.pdf<br><br>Guidelines for System Hardening:<br><br>📄 PDF<br><br>15. ISM - Guidelines for System Hardening |
| 29 | 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. | **1.** Organisation shall review default system configurations and rectify weak settings before deploying the assets, *i.e.,* Organisation shall always change the passwords of default accounts and disable default accounts where possible, to prevent risk of attack using default account and password. | |
| 30 | 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 | **2.** Organisation shall adopt hardening guidelines for system, operating system and devices from industry best practices such as CIS, Cloud Security Alliance, etc. | |

| S/N | (A)<br>MOH HIB requirements | Guidelines for HIB Guidebook | | |
| --- | --- | --- | --- | --- |
| | | (B)<br>Explanation on MOH HIB Requirements | | (C)<br>Help and Resources |
| | Equivalent Privacy (WEP) to Wi-Fi Protected Access 2/3 (WPA2/WPA3) to enhance the Wi-Fi security standards. | | | |
| 31 | 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. | | | |
| 32 | 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. | | | |
| | **[5] Back up: Back up essential data and store them offline** | | | |
| 33 | 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 | **1.** Organisation shall develop a backup policy which includes reviews of their systems and determine what systems are business critical and important to their operations.<br><br>**2.** Organisation shall back up their critical data into storage devices such as network storage servers or into a separate secure hard disk.<br><br>**3.** Organisation shall determine the backup frequency after reviewing operational requirements.<br><br>Organisation shall take into consideration, the impact to their operation during system downtime or cybersecurity incident when determining the backup frequency.<br><br>**4.** Organisation shall document the type of data to be backed up, frequency of the backup and define procedure to support business continuity during disruption | | |
| 34 | 5.44 The backups shall be performed on a regular basis, with the backup frequency aligned to the business requirements and | Organisation shall establish a recovery point objective (RPO) to allow days of data to be lost/recreated if necessary. | | *Recovery Point Objective (RPO):*<br>*The point in time to which data must be recovered after an outage.* |

| S/N | (A)<br>MOH HIB requirements | Guidelines for HIB Guidebook | |
|---|---|---|---|
| | | (B)<br>Explanation on MOH HIB Requirements | (C)<br>Help and Resources |
| | how many days' worth of data they can afford to lose. | RPO should be established with consensus between business, IT and Management.<br><br>The establishment of the RPO will help to determine the frequency and backup types. | |
| 35 | 5.45 If the scope includes cloud environment, the healthcare provider shall:<br><br>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<br>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. | **1.** Organisation shall establish clarity of their roles and responsibilities when using cloud services.<br><br>**2.** The cloud provider's roles and responsibilities shall be clearly defined in the contract with an established service level agreement.<br><br>*Example:*<br>- *Who is responsible for data backup and restoration*<br>- *Backup frequency*<br>- *Restoration verification*<br><br>**3.** Organisation shall back up their critical data into a storage devices such as network storage server or into a separate secure hard disk. | |
| 36 | 5.46 All backups shall be protected from unauthorised access and be restricted to authorised personnel only. Backups should minimally be password-protected. | Organisation shall protect backups from unauthorised access through means of password protection. | |
| 37 | 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. | **1.** Organisation shall maintain backups offline, ensuring they are not connected to the same network. Where feasible, backups should be stored offsite, in a separate location from operating site.<br><br>**2.**When operating in cloud environment or backup to cloud, | |
| 38 | 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 | Organisation shall ensure that data security and privacy are enforced. Where possible, cloud backup should enforce logical separation. Organisation shall ensure service level agreement and requirements are contractually bound with the cloud service provider.<br><br>*Example:* | |

| S/N | (A)<br>MOH HIB requirements | Guidelines for HIB Guidebook | |
|---|---|---|---|
| | | (B)<br>Explanation on MOH HIB Requirements | (C)<br>Help and Resources |
| | external hard disks and/or tape storage at an alternative office location | *If the main site is in datacentre 1, the backup site should be in datacentre 2.* | |
| 39 | 5.49 Backups shall be tested annually, or more frequently, to ensure that business-critical systems and essential business information can be restored effectively | **1.** Organisation shall develop data recovery procedures.<br><br>**2.** Data recovery testing is to be performed at minimum annually<br><br>**3.** The data recovery procedures and frequency shall be clearly documented. | |
| | **[6] Asset: People – equip staff with cyber-hygiene practices as the first line of defence** | | |
| 40 | 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. | **1.** Organisation shall ensure personnel (i.e., full time / part time staff, interns, contractors, vendors) who have access to the organisation's network/systems are briefed and trained on cybersecurity awareness.<br><br>**2.** The cybersecurity training shall minimally include Cyber & Data good practices via self-learning, external training provider or internal training.<br><br>**3.** Organisation shall document the frequency of the training and maintain records of the briefings and trainings attended by staff. | Sample Acceptable Use of Technology Resources Policy<br><br>📄 PDF<br><br>Acceptable-Use-of-Information-Technology |
| 41 | 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 | The cybersecurity awareness program shall at minimum include topics, such as:<br><br>a) phishing awareness and impact,<br><br>b) use of strong passphrase, | Sample Security Awareness and Training Policy:<br><br>📄 PDF<br><br>Security-Awareness-and-Training-Policy.d |

| S/N | (A)<br>MOH HIB requirements | Guidelines for HIB Guidebook | | |
| --- | --- | --- | --- | --- |
| | | (B)<br>Explanation on MOH HIB Requirements | | (C)<br>Help and Resources |
| | incidents arising from the human factor. Table 2 lists examples of measures that can be considered for developing cyber hygiene practices and guidelines:<br><br>i.     Protect yourself from phishing;<br>ii.    Set strong passphrase as passwords;<br>iii.   Protect your corporate and/or personal devices (used for work);<br>iv.   Report cyber incidents;<br>v.    Handle and disclose business-critical10 data carefully; and<br>vi.   Work onsite and remotely in a secure manner | c) BYOD usage,<br><br>d) reporting of suspicious activities or incident,<br><br>e) managing sensitive data.<br><br>f) risks of using public WiFi<br><br><br>*Examples of implementing cybersecurity awareness can be:*<br>- *Screen savers*<br>- *Email bulletins*<br>- *Posters* | | |
| 42 | 5.54 For more information, please refer to CSA's Cybersecurity Toolkit for Employees). | | | Cybersecurity Toolkit for Employees from CSA:<br><br>📄 PDF<br><br>CSA_SGCyberSafe_Employees-Toolkit_202 |
| | [7] Asset: Hardware and Software – Identify the hardware and software used in your organisation, and protect them | | | |
| 43 | 5.56 Healthcare providers shall maintain an up-to-date inventory of assets used in the healthcare provider for:<br>i.    All hardware (e.g., medical devices, Personal Computer (PCs), laptops, printers, modems, and network routers); and<br>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 software or tools) | **1.** Organisation shall create and maintain a software and hardware assets inventory list to effectively manage their assets.<br><br>**2.** The inventory should be reviewed and updated regularly to ensure accuracy and completeness.<br><br>**3.** The inventory should capture information related to hardware and software use, version, and where possible the End of Life (EOL) information. | | Sample inventory list template:<br><br>📊<br><br>CIS_Hardware_and_Software_Asset_Trackir |

| S/N | (A)<br>MOH HIB requirements | Guidelines for HIB Guidebook | |
| --- | --- | --- | --- |
| | | (B)<br>Explanation on MOH HIB Requirements | (C)<br>Help and Resources |
| 44 | 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. | | |
| 45 | 5.58 The healthcare provider shall develop a protocol to authorise new hardware and software into the healthcare provider. 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 | **1.** Organisation shall develop an approval process where software and hardware assets are approved by management before onboarding for usage.<br><br>**2.** Such onboarding shall include SaaS solution/application as well.<br><br>**3.** As part of onboarding, the approved software and/or hardware assets shall be recorded accordingly in the inventory listing.<br><br>The inventory list shall at minimum include:<br>a) installed software version(s)<br>b) device model (for hardware)<br>c) owner<br>d) EOL information<br>e) approval documentation<br>f) location of installation | |
| 46 | 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 healthcare provider. Software and hardware without an approval date shall be removed | **4.** Organisation shall remove any unauthorised software and hardware without an approval date.<br><br>(For legacy* hardware and software, Organisation should consider a one-time review, and risk assessment and obtain approval from Management for continuous usage.)<br><br>* Hardware and software that have missing approval information | |
| 47 | 5.60 Software shall only be installed if needed on corporate devices. Any devices shall be disconnected and software to be | **1.** Organisation shall put in place processes to remove software and data from devices prior to disposing the hardware. | Sample Mobile Device Security Standard: |

| S/N | (A)<br>MOH HIB requirements | Guidelines for HIB Guidebook | |
|---|---|---|---|
| | | (B)<br>Explanation on MOH HIB Requirements | (C)<br>Help and Resources |
| | 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 | **2.** Organisation shall use mobile device management (MDM) when allowing BYOD or mobile devices to access patient and sensitive corporate information, to allow remote wipe of the data when the device is lost or resignation of the staff. | [PDF icon]<br>Mobile-Device-Security.docx_safe (1).pdf |
| 48 | 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 | Organisation shall put in place a procedure or policy to replace End of Support (EOS) hardware and software assets in a timely manner to prevent unnecessary support or exploitation of vulnerabilities.<br><br>If there a need to continue to use the EOS assets, organisation shall perform impact and risk assessment to determine the implication to the organisation and assess whether the risk can be accepted by management. | |
| 49 | 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 | Risks that have been accepted by management should be tracked and monitored closely. | |
| | **[8] Asset: Data – Identify the types of data your organisation has, where they are stored, and secure them** | | |
| 50 | 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) | **1.** Organisation shall put in place a procedure or policy to establish data classification of the organization's data assets/inventory.<br><br>**2.** The data classification shall take into consideration, the business impact and risk affecting organisation if the data is lost, unavailable or unrecoverable.<br><br>**3.** Organisation shall establish the necessary measures to protect their data from unauthorized access.<br><br>*Example of such measures are: a) use of password/passphrase* | |
| 51 | 5.65 The policies and processes shall also include measures to prevent employees from | *b) disabling of USB* | |

| S/N | (A)<br>MOH HIB requirements | Guidelines for HIB Guidebook | |
| --- | --- | --- | --- |
| | | (B)<br>Explanation on MOH HIB Requirements | (C)<br>Help and Resources |
| | leaking confidential and / or sensitive data outside of the healthcare provider. This requirement may be met in different ways e.g., controlled access, disabling USB ports | *c) using solution such as data loss prevention software*<br><br>*d) use of encrypted portal portable hard disk*<br><br>**4.** Organisation shall establish a process to review users' access to business' critical data and systems.<br><br>**5.** When access is no longer required, user access shall be removed from the system/application. | |

## 2. Data Security Guidebook

| S/N | (A)<br>MOH HIB requirements | Guidelines for HIB Guidebook | |
| --- | --- | --- | --- |
| | | (B)<br>Explanation on HIB Requirements | (C)<br>Help and Resources |
| | [9] Secure: Storage Requirements – Store your health information securely to prevent unauthorised access | | |
| 52 | 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. | **1.** The retention period of classified health information shall be clearly defined within the data retention policy.<br><br>**2.** Service provider shall take reference from the below retention policies:<br>**-** MOH issued national guidelines for retention periods of medical records. | Organisations may refer to the following resources:<br>1. MOH National Guidelines for Retention Periods of Medical Records<br><br>2. PDPC Advisory Guidelines for The Retention Limitation Obligation |

DATA SECURITY

| S/N | (A)<br>MOH HIB requirements | Guidelines for HIB Guidebook | |
| --- | --- | --- | --- |
| | | (B)<br>Explanation on HIB Requirements | (C)<br>Help and Resources |
| 53 | 6.4 Healthcare providers shall ensure that Sensitive Normal / Sensitive High health information is secured from unauthorised access or loss, as follows:<br><br>**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.<br><br>**ii.** Where healthcare providers use commercial storage facilities, healthcare providers shall ensure the following:<br><br>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);<br><br>b. Maintain proper records to indicate materials containing sensitive data deposited in offsite storage; and<br><br>c. Conduct audits to ensure materials are intact or in order and have not been subject to unauthorised access. | **1.** The organisation shall have in place an appropriate security policy to secure classified health information in its possession or under its control from unauthorised access or from loss.<br><br>Examples to secure health information includes but not limited to:<br>a. **Hardcopy documents**<br>Copies of Sensitive Normal / Sensitive High health information shall be secured via physical measures such as:<br>• Storing in locked file cabinets / filing rooms with restricted access<br>• Office premises shall only be accessed by authorised personnel (e.g. secured access via lock and key, biometric access, security gantries).<br>• Sensitive documents shall not be left unattended and in the open when not in use.<br>b. **Softcopy documents**:<br>Health information held digitally shall be secured in manners such as:<br>• Desktop PCs and laptops shall be physically secured within the office premises (e.g. cable-lock).<br>• Access to files containing sensitive health information shall be restricted through measures such as password protection or placing files in access restricted folders.<br><br>**2.** When engaging a third party to store health information (e.g. commercial storage facilities, client management systems, cloud storage platforms), the organisation shall minimally have in place the following controls:<br>a. Vendor shall through contractual obligations (e.g., agreements, terms of use, data protection policy etc) be required to manage data in accordance with prevailing legislations, policies or standards (e.g., PDPA)<br><br>b. The organisation shall maintain an inventory of health information stored with a third party, and conduct periodic reviews on the integrity of health information (e.g. review access logs of softcopy files stored in the cloud, verify physical documents in storage sites). | Organisations may refer to the following guides for securing Health Information:<br>1. PDPC's guide to securing personal data in electronic medium<br><br>2. To maintain an inventory of Health Information stored offsite, organisations may refer to PDPC's sample Personal Data Inventory Map Template. |

| S/N | (A)<br>MOH HIB requirements | Guidelines for HIB Guidebook | |
|---|---|---|---|
| | | (B)<br>Explanation on HIB Requirements | (C)<br>Help and Resources |
| **[10] Secure: Reproduction Requirements – Do not reproduce copies of sensitive health information unless necessary** | | |

| S/N | (A)<br>MOH HIB requirements | (B)<br>Explanation on HIB Requirements | (C)<br>Help and Resources |
|---|---|---|---|
| | **[10] Secure: Reproduction Requirements – Do not reproduce copies of sensitive health information unless necessary** | | |
| 54 | 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. | **1.** This applies to scenarios where copies of sensitive Health Information are made.<br><br>Examples include but not limited to the following:<br>a. Copies made on photocopiers, fax machines, scanners and multi-functional devices<br>b. Copies made on portable storage devices such as thumb drive and hard drives<br><br>**2.** The organisation shall have <u>appropriate corporate policies</u> to cater for scenarios where copies can be made on a <u>need-to-know basis</u>.<br><br>Corporate policies shall also <u>define the procedures</u> to secure and prevent:<br>a. unauthorised access to copies of sensitive Health Information; and<br>b. the loss of copies of sensitive Health Information where they are managed by the organisation or a third party engaged by the organisation. | Organisations may refer to the following guides for securing Health Information:<br>1. PDPC's guide to securing personal data in electronic medium |
| 55 | 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). | | |
| | **[11] Secure: Conveyance Requirements – Transport health information properly to avoid unwanted data exposure** | | |
| 56 | 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:<br><br>i. Its personnel do not carry health information to locations for non-work purposes;<br>ii. The materials are kept in its personnel's possession / control at all times; | **1.**The organisation shall have <u>appropriate corporate policies</u> defining the procedures for transferring sensitive Health Information in a secured manner to prevent unauthorised access and loss of information.<br><br>**2.**This applies to scenarios where carrying physical Sensitive Normal / Sensitive High health information outside of the permitted work areas is unavoidable, the <u>appropriate precautions shall be taken to prevent any accidental loss of information</u>. Similarly, where sensitive Health Information needs to be transmitted electronically, <u>procedures</u> shall be in place to minimise data loss. | Organisations may refer to the following guides for securing Health Information:<br>1. PDPC's guide to securing personal data in electronic medium<br><br>2. PDPC's guides on Data Protection Management Programme and Data Protection Impact Assessment. |

| S/N | (A)<br>MOH HIB requirements | Guidelines for HIB Guidebook | |
|---|---|---|---|
| | | (B)<br>Explanation on HIB Requirements | (C)<br>Help and Resources |
| | iii. The health information is prevented from accidental exposure (e.g., where another person can see the information in plain sight); and<br>iv. When transmitting health information electronically, e.g., by email, the files are password-protected and are sent to the right recipients.<br><br>For more information, please refer to the PDPC guides on Data Protection Management Programme and Data Protection Impact Assessment. | | 3. CSA's guide on how to create a strong password |
| | **[12] Identify: Data Security Classification – Know the information sensitivity levels of the data to apply appropriate safeguards** | | |
| 57 | 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.<br><br>For more information, please refer to PDPC's Guides on Data Protection Management Programme and Data Protection Impact Assessment. | As organisations may collect a wide variety of information, they are required to have a data classification policy in place to identify health information in its possession and subsequently classify them. This enables the organisation to differentiate Non-Sensitive information from Sensitive Normal / Sensitive high health information that are subjected to the various requirements stated within this guide.<br><br>Classification of health information shall be applied in accordance with Table 4:<br><br>Table 4: Data Classification and Examples of Data Types<br><br>| Data Classification | Examples of Data Types[18] |<br>|---|---|<br>| Non-Sensitive | • Anonymised Data (i.e., cannot be associated with specific individuals.) |<br>| Sensitive Normal | • General Health Information<br>• Medical/Lab Reports<br>• Discharge Summaries<br>• Genomic Information (excluding Whole Genome and/or Whole Exome Sequences)<br>• Demographics Information, e.g., race, ethnicity |<br>| Sensitive High | • Sensitive Health Information (e.g., HIV, mental disorders such as schizophrenia, delusional disorders, substance abuse and addictions).<br><br>_<Please refer to the MOH corporate website for the full list.>_ | | Organisations may refer to PDPC's Guide to Basic Anonymisation on how to anonymise health information for it to be classified as Non-Sensitive.<br><br>Other relevant PDPC guides:<br>a. Data Protection Management Programme<br>b. Data Protection Impact Assessments<br><br>_List of Sensitive Health Information to be classified as Sensitive-High can already be found in Table 4._ |

DATA SECURITY

| S/N | (A)<br>MOH HIB requirements | Guidelines for HIB Guidebook | |
| --- | --- | --- | --- |
| | | (B)<br>Explanation on HIB Requirements | (C)<br>Help and Resources |
| 58 | 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. | The data classification policy shall have provisions for records containing various classified health information to be tagged at the highest level.<br><br>For example, patient referral forms may contain demographic data and health conditions such as mental disorders. Information on mental disorders fall under the classification of Sensitive High, hence the patient referral form shall be classified as Sensitive High. | |
| 59 | 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. | Data classifications may also change over time (e.g. types of data listed in the SHI list may change). To address this, the organisation's data classification policy shall have provisions to review and alter data classifications in line with MOH's policy. | Organisations may refer to the Prescribed Classes of Medical Information in PDPA Regulations for the list of Sensitive Health Information. |

DATA SECURITY

| S/N | (A) MOH HIB requirements | Guidelines for HIB Guidebook | |
|---|---|---|---|
| | | (B) Explanation on HIB Requirements | (C) Help and Resources |
| 60 | 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:<br>i. **Type and description of data** e.g., clinical assessment forms, patient referral forms, patient medical records;<br>ii. **Sensitivity classification of data** e.g., Sensitive Normal or Sensitive High based on the highest classification imposed;<br>iii. **Medium the data resides as** e.g., hardcopy records, electronic records;<br>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;<br>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<br>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, 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. | While organisations collect and classify vast amounts of health information, they shall have a data security policy to maintain an updated data inventory of health information to capture information stated in the requirements.<br><br>Data Inventory Map fields shall contain the following:<br>1) Type and description of data<br>2) Sensitivity classification of data<br>3) Medium the data resides as<br>4) Storage of data<br>5) Retention period<br>6) Disposal method | Organisations may refer to the following PDPC materials for more information:<br>1. PDPC's Sample of Personal Data Inventory Map Template<br>2. PDPC's Sample of Data Flow Illustration |

| S/N | (A)<br>MOH HIB requirements | Guidelines for HIB Guidebook | |
|---|---|---|---|
| | | (B)<br>Explanation on HIB Requirements | (C)<br>Help and Resources |
| | [13] Identify: Marking Requirements – Differentiate data of varying information sensitivity levels by marking their classification | | |
| 61 | 6.20 The healthcare provider shall have policies in place for the marking of Sensitive Normal / Sensitive High health information to enable its staff to recognise 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.<br><br>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. | To enable easier identification of classified health information, organisations shall have an appropriate marking policy that requires all hardcopy and softcopy documents containing Sensitive Normal / Sensitive High health information to be marked with the corresponding data security classification.<br><br>For scenarios where it is impractical to mark a record / document, the marking policy shall stipulate that "the record / document within the organisation is classified as Sensitive High". Examples of such scenarios include:<br>  a) An external document containing health information brought in by a patient / client.<br>  b) Notes containing health information documented outside of standardised forms or templates. | |

DATA SECURITY

| S/N | (A)<br>MOH HIB requirements | Guidelines for HIB Guidebook | |
| --- | --- | --- | --- |
| | | (B)<br>Explanation on HIB Requirements | (C)<br>Help and Resources |
| | [14] Access: Authorised Users – Restrict access to health information for valid and relevant purposes | | |
| 62 | 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:<br><br>i. **Need-to-Know**: Staff 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).<br><br>ii. **Data Security-Briefed**: Staff have been informed or made aware of and acknowledged the data protection and security requirements in these Guidelines and prevailing laws e.g., PDPA, and / or healthcare provider's corporate policies. | **1.** Access to classified health information shall be <u>governed by a data security policy</u> to protect against unauthorised access. The policy shall state an approval process for granting access to health information if the staff meets the following:<br><br>a. Need-to-know<br>b. Data Security-Briefed<br>    *refer to Col A for explanatory note on the conditions.<br>c. Acknowledgement capturing should be done via a Letter of Undertaking or its equivalent on all staff (including volunteers)<br><br>**2.** This means that organisations should not grant their staff access to health information on a '*just in case*' basis. | |

# 3. Common Cyber and Data Security Guidebook

| S/N | (A)<br>MOH HIB requirements | Guidelines for HIB Guidebook | |
|---|---|---|---|
| | | (B)<br>Explanation on HIB Requirements | (C)<br>Help and Resources |
| | [15] Outsourcing & Vendor Management: Understand the responsibilities set between your organisation and vendor | | |
| 63 | 7.2 If healthcare providers are using an IT service provider to manage their network, systems, and medical devices, they shall:<br><br>i.   Clearly understand the services and security practices that the IT service provider will provide; and<br><br>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. | **1.** Organisations that engage external IT service providers to manage their IT infrastructure (e.g., network, IT systems, medical devices) <u>shall have a process to assess the vendors on criteria</u> such as but not limited to:<br>  a.  Does the vendor regularly keep up to date with new cyber threats;<br><br>  b.  Does the vendor have any cybersecurity certification (e.g., CSA Cyber Trust Mark);<br><br>  c.  Are there regular trainings provided by the vendor to their employees;<br><br>  d.  Does the vendor have any breach management / cybersecurity incident plan and prep for such scenarios through simulation exercises as an example.<br><br>**2.** Organisations <u>should not</u> engage IT service providers solely on which provider may have quoted the lowest cost.<br><br>**3.** Organisation shall establish clear roles and responsibilities with their IT service providers and document this clearly in the contract.<br><br>**4.** The scope of the contract shall include:<br>  a.  Security Management and Practices;<br>  b.  Vulnerabilities and Patch management;<br>  c.  Regular meeting on issues and problem management where applicable. | |

| S/N | (A)<br>MOH HIB requirements | Guidelines for HIB Guidebook | |
|---|---|---|---|
| | | (B)<br>Explanation on HIB Requirements | (C)<br>Help and Resources |
| 64 | 7.3 When using third-party software and devices, healthcare providers shall:<br><br>i. Ensure that they clearly understand:<br>   a. How patient and corporate data is processed, transferred, and stored;<br>   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);<br>   c. What the contractual arrangements with vendors are, including responsibilities of each contractual party in the event of an incident or breach; and<br><br>ii. Subscribe to security-related alerts published by vendors for the third-party software and devices their practice uses. | 1. Prior to engaging a third-party vendor to provide software and devices, the organisation shall have a process to understand how health information and corporate data will be handled by the vendor.<br>Considerations include but will not be limited to:<br>   a. How many of the vendor's staff will have access to the information.<br>   b. Will data be stored locally or outside of Singapore.<br>2. Organisations may also refer to the examples of assessment criteria in row 12 to assess the vendor's security practices and safeguards that they may have in place.<br><br>3. Organisations shall enter into contractual agreements with the vendors providing such software / devices. The contract shall minimally stipulate the responsibilities of each party in the event of an incident or breach.<br><br>4. Organisation shall include in the contractual agreements with vendors that the vendors need to carry out review on patching and refresh software and hardware in a timely manner to provide assurance.<br><br>5. Organisation shall establish processes to monitor their software use for security alerts through subscribing to known security alert portals. | Organisations may refer to the following materials from PDPC for more information:<br>1. When transferring data out of Singapore, the organisation may refer to the Advisory Guideline on The Transfer Limitation Obligation for consideration<br>2. PDPC's Guide to Data Protection Practices for ICT Systems |

| S/N | (A)<br>MOH HIB requirements | Guidelines for HIB Guidebook | |
| --- | --- | --- | --- |
| | | (B)<br>Explanation on HIB Requirements | (C)<br>Help and Resources |
| 65 | 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. | **1.** Organisation using cloud services shall define and understand the responsibilities between the cloud provider and organisation and/or organisation selected vendor.<br><br>For example:<br>AWS is responsible for the infrastructure and OS patching while the vendor or organisation is responsible for the application patching.<br><br>**2.** When using cloud services, the organisation shall have in place a cybersecurity policy to ensure that key responsibilities are assigned to relevant staff who are aware that they are in charge of managing the use of the cloud service.<br><br>For example:<br>a. Appointing a staff to be responsible for overseeing the use of the cloud service (e.g., IT Dept Head).<br><br>b. Which staff(s) should have access to the cloud service via password login/cryptographic keys.<br><br>c. Staff(s) responsible for prompting review of user access and permissions to the cloud service to remove/edit user's access when no longer needed in a timely manner. | For more information on using cloud services and cloud security, organisations may refer to CSA's Cloud Security for Organisations programme and to the Chapter on Cloud Services in PDPC's Advisory Guidelines on Selected Topics (Chapter on Cloud Services). |

| S/N | (A)<br>MOH HIB requirements | Guidelines for HIB Guidebook | |
| --- | --- | --- | --- |
| | | (B)<br>Explanation on HIB Requirements | (C)<br>Help and Resources |
| 66 | 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.<br><br>For more information, please refer to the Chapter on Cloud Services in PDPC's Advisory Guidelines on Selected Topics (Chapter on Cloud Services). | 1. Organisation shall conduct an assessment, <u>documenting its considerations on the risk and impact</u> when storing sensitive health information online or through third-party products and services.<br><br>2. If sensitive data is stored in the cloud, evaluation considerations such as risk associated, accountabilities, legal oversight implication, legislation oversight shall be incorporated into the <u>contractual agreement</u> to safeguard the organisation where possible.<br><br>3. Organisation shall refrain from engaging services found to be unsafe or have potentially high risk for the organisation.<br><br>4. Organisations shall have a <u>process to conduct a background assessment</u> of the IT service provider or vendor that provide the third-party software to gauge their credibility and reliability before procuring third party product services. For example, taking into consideration:<br>  a. Organisation may research if the vendor had past data breaches (e.g., via PDPC's enforcement decisions). Vendors with a bad track record should be avoided when possible.<br>  b. Organisations may request for vendors to disclose if they had past cybersecurity incidents that was reported to SingCERT (CSA), and if so, has there been remedial actions put in place to prevent similar future incidents.<br>  c. Organisations can request for vendors to share their past experiences in providing their products / services.<br>  d. For cloud service providers, review vendor's certifications such as if they've attained ISO27001, or Tier 3 of the Multi-Tiered Cloud Security (MTCS) Certification Scheme | For more information on using cloud services and cloud security, organisations may refer to CSA's Cloud Security for Organisations programme. |

| S/N | (A)<br>MOH HIB requirements | Guidelines for HIB Guidebook | |
| --- | --- | --- | --- |
| | | (B)<br>Explanation on HIB Requirements | (C)<br>Help and Resources |
| | **[16] Incident Response: Prepared to detect, respond, and recover from incidents** | | |
| 67 | 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).<br><br>Examples include, e.g., phishing, ransomware, and data breach. The plan shall contain the following details:<br><br>i.  Clear roles and responsibilities of key personnel in the healthcare provider involved in the incident response process;<br><br>ii.  Procedures to detect, respond, and recover from the common cyber / data threat scenarios, e.g., phishing, ransomware, data breach; and<br><br>iii.  Communication plan and timeline to escalate and report the incident to internal and external stakeholders (such as regulators, customers, and senior management). | **1.** The organisation shall document an incident management and response plan, including procedures that enable the organisation to manage and respond to breaches effectively. For example, roles and responsibilities shall be clearly defined and documented in the incident response and management process/policy.<br><br>**2.** The organisation shall take reference on the reporting requirements as issued from MOH. For example, the reporting thresholds and timelines summarised in Table 5. The 2 hour timeline is from the point of the organisation determining that there is a notifiable data breach in accordance with PDPC's definition of Data Breach Notification Obligation.<br><br>**3.** The incident response and management process/policy shall be reviewed annually or at a frequency determined by management and/or when there are changes in policy, for examples, new regulatory requirements or change or introduction of a new system or services. | Organisations may refer to the following guides:<br>1.  PDPC's guide on managing and notifying data breaches<br><br>2.  CSA's Incident Response Checklist<br><br>Incident-Response-Policy.docx<br><br>3. |

| S/N | (A)<br>MOH HIB requirements | Guidelines for HIB Guidebook | |
|---|---|---|---|
| | | (B)<br>Explanation on HIB Requirements | (C)<br>Help and Resources |
| 68 | 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. | *<Note: The proposed incident reporting thresholds and timelines for cyber or data incidents under the HIB 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.>*<br><br>Table 5: Proposed Incident Reporting Thresholds & Timelines under the HIB<br><br>| | Cybersecurity Incidents | Data Breaches |<br>|---|---|---|<br>| Reporting Thresholds | • A notifiable [23] cybersecurity incident involves:<br>i. a computer or computer system containing health information or interconnected with a computer or computer system containing health information; and<br>ii. The computer or computer systems are under the healthcare provider's control. | • Aligned to PDPA's data breach notification threshold.<br>• In the context of health information, a notifiable data breach is one that:<br>i. results in, or is likely to result in, significant harm to an affected individual (i.e., breach contains sensitive health information); or<br>ii. is, or is likely to be, of a significant scale (i.e., impact on equal or more than 500 affected individuals). |<br>| 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.<br>• Affected healthcare provider to provide an incident report within 14 days of initial notification.<br>• 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. | |<br><br>4. The organisation shall reinforce awareness of the incident management and reporting processes to report incidents that meet prevailing legislations, policies or standards (e.g., PDPA).<br><br>5. The organisation shall develop and communicate their incident reporting, incident response and management process/policy to all staff. For example, staff can be made aware of and be familiar with the incident response plan through annual briefing, e-learning, face-to-face trainings, newsletters, tabletop exercises and/or information that can found easily on the organisation's intranet. | |

| S/N | (A)<br>MOH HIB requirements | Guidelines for HIB Guidebook | |
|---|---|---|---|
| | | (B)<br>Explanation on HIB Requirements | (C)<br>Help and Resources |
| | [17] Disposal Requirements: Proper disposal of health information mitigates the risk of unauthorised access | | |
| 69 | 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). | 1. The organisation shall have <u>corporate policies or processes on how data, including sensitive health information (physical or digital), is disposed securely</u> after the retention period expires or when there is no longer any business / legal needs for retention.<br><br>For example,<br><br>a. Physical media such as paper, CD, DVD, etc. shall be shredded/destroyed prior to disposal.<br><br>b. Off-the-shelf software solutions, such as kill disk and disk wipe to securely erase the data in storage hard drive such as portable HDD, USB thumb drives, network storage shall be used prior to disposal and/or physically destroyed. Example of physical destruction can be:<br>  i.  Drilling through<br>  ii.  Mechanical shredding<br><br>  d.  Organisations may consider engaging a secure disposal vendor for hardware asset disposal. A certificate of secure disposal shall be provided by the vendor upon disposal and documented. | Organisations may refer to the following guides for disposing Health Information:<br>1.  PDPC's guide to securing personal data in electronic medium<br><br>2.  PDPC's guide to disposal of personal data on physical medium<br><br><br>Sample Sanitization/Secure Disposal Standards from NIST:<br><br>📄 PDF<br>Sanitization-Secure-Disposal-Standard.do<br><br><br>Guidelines for Media Sanitization from NIST:<br><br>SP 800-88 Rev. 1, Guidelines for Media Sanitization \| CSRC (nist.gov) |

| S/N | (A)<br>MOH HIB requirements | Guidelines for HIB Guidebook | |
| --- | --- | --- | --- |
| | | (B)<br>Explanation on HIB Requirements | (C)<br>Help and Resources |
| | **[18] Emergency Planning for Contingency: Supports ability to withstand service disruptions to ensure business continuity** | | |
| 70 | 7.14 The healthcare provider shall:<br><br>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.<br><br>ii.   Regularly review the relevance and test the effectiveness of the organisation's business continuity plan through planned scenario-based training or exercises. | **1.** The organisation shall <u>develop contingency plans for common business disruption scenarios</u> caused by cyber and data incidents to ensure there is minimal disruption to services provided by the organisation<br><br>**2.** The organisation shall <u>conduct regular tabletop or simulation exercises</u> which involves triggering of contingency plans to review their effectiveness, ensuring that staff are familiar with the plans to continue operating during recovery process.<br><br>**3.** Testing scenarios should include when major systems may not be available or outage from a few hours to potentially days or weeks.<br><br>**4.** The organisation shall review and update the business continuity plan regularly or when there are major changes in the organisation. | Organisations may refer to the following guides:<br>1.  PDPC's guide on managing and notifying data breaches |

| S/N | (A)<br>MOH HIB requirements | Guidelines for HIB Guidebook | |
| --- | --- | --- | --- |
| | | (B)<br>Explanation on HIB Requirements | (C)<br>Help and Resources |
| | **[19] Review Security & Internal Audit Requirements: Regular checks on corporate policies and processes to ensure compliance and identify vulnerabilities** | | |
| 71 | 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). | **1**. The organisation shall put in place <u>a process to conduct checks</u> on their cyber and data security safeguards placed on sensitive Health Information to identify potential vulnerabilities. For example, self-assessment health checks shall be established to review and identify compliance gaps to policies/processes or regulatory requirements.<br><br>**2**. Where there are vulnerabilities or compliance gaps identified, the organisation shall have <u>a process to take corrective actions as soon as possible to improve compliance.</u> Corrective actions shall include action plans approved by senior management. | Organisations may refer to the <u>PDPC's guide on Data Protection Management Programme and Data Protection Impact Assessment.</u> |

CYBER AND DATA SECURITY