# Health Information Act: Practical Steps Towards HIA Readiness


| | Content Page | Slide |
|---|---|---|
| 1 | NEHR Checklist and Preparations | 2 to 8 |
| 2 | Cybersecurity and Data Security (CS/DS) Measures under the Health Information Act (HIA) | 9 to 29 |
| 3 | Contact Us | 30 |




MINISTRY OF HEALTH
SINGAPORE



# NEHR Checklist and Preparations

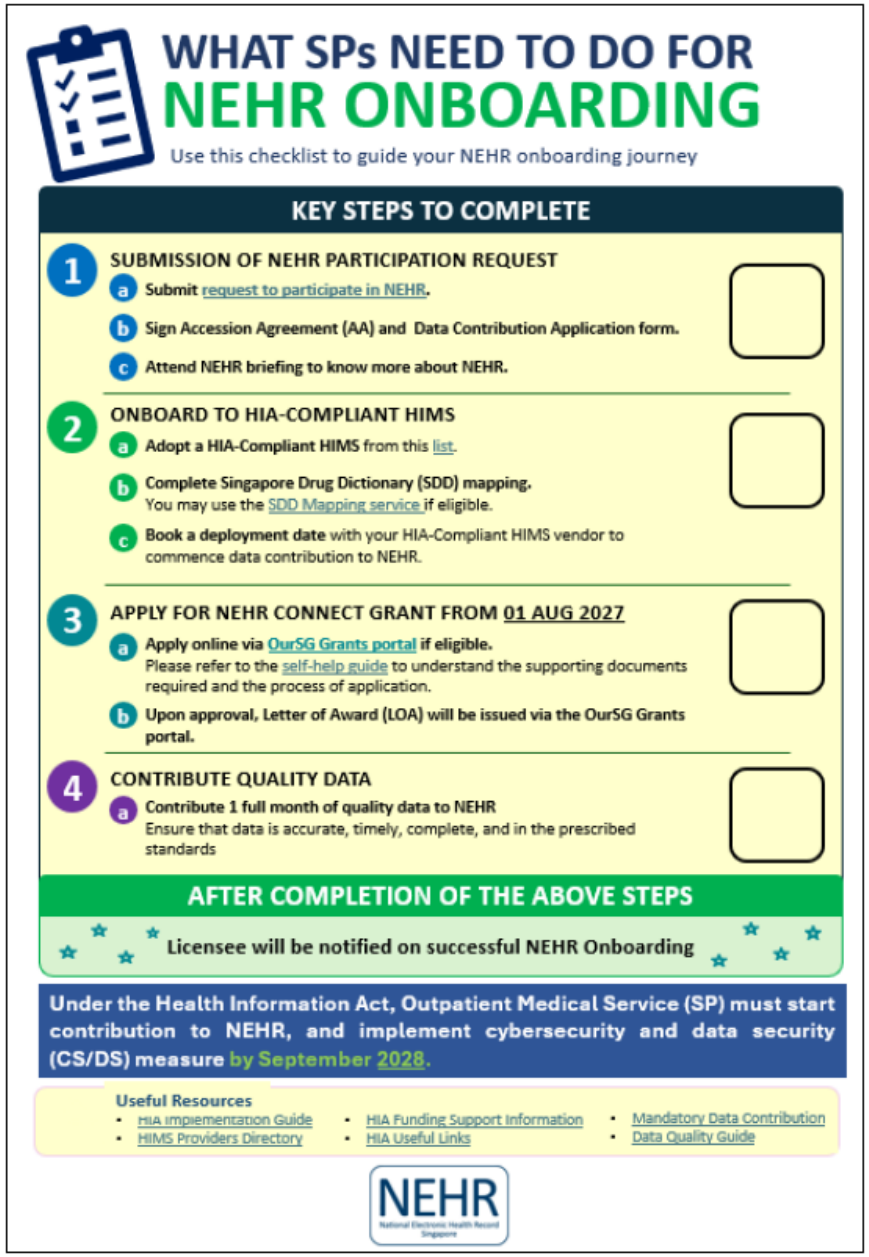
Healthier SG
An initiative of
FORWARD SG

# What does mandatory contribution to NEHR mean?

synapxe

- Under the **Health Information Act (HIA)**, all licensed healthcare providers and retail pharmacies must contribute key health information to the NEHR.
- Implementation is done in phases for different Licensable Healthcare Services, with **Outpatient Medical Service (SP) required to contribute data by Sept 2028.**
- Selected health information from your care episodes with your patients will need to be contributed seamlessly via a HIA-compliant Health Management System (HIMS) to the NEHR. This data will be stored in NEHR to enable
  - better care coordination across healthcare providers
  - fewer duplicated tests
  - Key health information available during emergencies

## What do you as an SP need to do to enable contribution of health information to NEHR?



WHAT SPs NEED TO DO FOR
NEHR ONBOARDING

Use this checklist to guide your NEHR onboarding journey

KEY STEPS TO COMPLETE

1 SUBMISSION OF NEHR PARTICIPATION REQUEST
- a Submit request to participate in NEHR.
- b Sign Accession Agreement (AA) and Data Contribution Application form.
- c Attend NEHR briefing to know more about NEHR.

2 ONBOARD TO HIA-COMPLIANT HIMS
- a Adopt a HIA-Compliant HIMS from this list.
- b Complete Singapore Drug Dictionary (SDD) mapping. You may use the SDD Mapping service if eligible.
- c Book a deployment date with your HIA-Compliant HIMS vendor to commence data contribution to NEHR.

3 APPLY FOR NEHR CONNECT GRANT FROM 01 AUG 2027
- a Apply online via OurSG Grants portal if eligible. Please refer to the self-help guide to understand the supporting documents required and the process of application.
- b Upon approval, Letter of Award (LOA) will be issued via the OurSG Grants portal.

4 CONTRIBUTE QUALITY DATA
- a Contribute 1 full month of quality data to NEHR. Ensure that data is accurate, timely, complete, and in the prescribed standards

AFTER COMPLETION OF THE ABOVE STEPS

Licensee will be notified on successful NEHR Onboarding

Under the Health Information Act, Outpatient Medical Service (SP) must start contribution to NEHR, and implement cybersecurity and data security (CS/DS) measure by September 2028.

Useful Resources
- HIA Implementation Guide
- HIMS Providers Directory
- HIA Funding Support Information
- HIA Useful Links
- Mandatory Data Contribution
- Data Quality Guide

NEHR

# Step 1: Submission of NEHR Participation Request

**1. Check your status of participation using this QR:**

**2. To participate in NEHR:**

Submit request to participate in NEHR or write to us at nehr.participation@synapxe.sg → We will reach out to you to prepare documentation to MOH which includes the Accession Agreement. → Receive MOH Approval → Apply for NEHR user account by emailing to nehr.svcops@synapxe.sg

To help you better understand the administrative responsibilities and answer any NEHR-related questions which you might have, you can register for a 30-minute virtual NEHR Onboarding briefing.

All registered medical practitioners are allowed to access the NEHR to provide healthcare services for their patients.

Should you need any assistance along the way, please reach out to nehr.feedback@synapxe.sg.

# Step 2: Onboard to a HIA-Compliant HIMS

synapxe

**Process to onboard to a HIA-Compliant HIMS:**

1. Adopt a HIA-Compliant HIMS
2. Complete Singapore Drug Dictionary (SDD) Mapping
3. Data Onboarding

- Check if your system is HIA-compliant using this link: https://for.sg/hchlist
- Adopt/Change to a HIA-compliant HIMS provider if your system is not HIA-compliant/not going to be HIA-compliant.

- You **must** map your clinic's drug inventory to SDD before onboarding.
- You can sign up for this optional SDD Workshop via this link.
- If required, you can sign up using link for drug mapping service. (Charges apply)

- Book a deployment date with your HIA-compliant HIMS provider to commence data contribution to NEHR.

**For more information on Drug Inventory Mapping, you can refer to the links below:**

- Standards briefing deck
- Video on SDD mapping
- FAQ on clinical standards

# Step 3: Apply for NEHR Connect Grant (NCG) from **1 Aug 27** once you decided on a HIA-Compliant HIMS

synapxe

## What is NEHR Connect Grant?

It is a funding support to help Licensable Healthcare Services in Singapore enhance their existing Health Information Management System or adopt one that can securely contribute data to the NEHR, in line with the HIA. **The quantum for OMS SP is $8,400.**
NCG funds are released only after onboarding, contribution, and passing one month of data quality assessment

## Who can apply?

Applicants for NCG must meet the following criteria:
1. Hold a valid HCSA licence or retail pharmacy license under the HPA.
2. Adopt or change to a HIA-compliant Health Information Management System (HIMS)
3. Have not previously received similar funding from MOH (such as GP ITE and NHELP) under the same HCI code.

## Process from application to payout:




### Apply for NCG

Login to OurSG Grants Portal and submit the mandatory documents to complete the NCG application.



### Sign the Letter of Award

Upon successful grant application, sign the LOA to accept the terms of the grant.



### Contribute under HIA

Submit the health information required under HIA to the NEHR through a HIA-compliant HIMS.



### Pass the Data Quality Assessment

Meet all 5 data quality criteria for one full month.



### Receive the NCG payout

# Step 4: Contribute Quality Data

Contribute 1 full month of quality data to NEHR. Ensure that data is accurate, timely, complete, and in the prescribed standards

1. The types of health information to be contributed varies by license and service provided. For outpatient medical services, health information that needs to be contributed includes:

- ✓ Visit Event
- ✓ Adverse Drug Event History
- ✓ Ordered (prescribed) Medications
- ✓ Dispensed Medications
- ✓ Visit Diagnoses or Patient Problem list
- ✓ Vaccines Administered

Full details can be found in the First Schedule of HIA.

2. Pass all data quality criteria

| # | Data Quality Criteria | Target for the Criteria | What it means |
|---|---|---|---|
| 1 | Timeliness | Passing Rate: 90% | Submit data within 72 hours to NEHR after the data is created or after the patient's clinical encounter. |
| 2 | Message Acceptance | Passing Rate: 95% | Submitted patient records must be accepted by NEHR. Refer to the published NEHR interface specifications and implementation guides to ensure that all data contribution requirements are met. |
| 3 | Reason for Visit Completeness | Passing Rate: 80% | Ensure that all visits have a reason for visit submitted through diagnosis information and/or discharge summary information. |
| 4 | Standards Compliance | Passing Rate: 70% | Patient records meet national coding standards for diagnosis, medication and laboratory results. |
| 5 | Demographics Accuracy | Passing Rate: 90% | Patient demographic information (such as sex and date of birth) must be accurate and matched to the correct patient. |

# Onboarding Confirmation and Self-help Resources

- Upon completing the key steps 1 – 4, you will be notified of **successful onboarding** to NEHR via email.

Scan QR code here




https://for.sg/nehrwebsite

You can visit our website (https://for.sg/connectnehr) for self-service support on mandatory data contribution, NEHR Connect Grant and useful links.

## ConnectNEHR

*Self-service portal for Healthcare and HIMS Providers*

- ☑ Latest updates to support a smooth NEHR onboarding journey
- ☑ Resources, guides, and supporting materials in one place

## AskNEHR

*Available at ConnectNEHR website. Powered by GenAI.*

- ☑ Quick, convenient answers to onboarding, contribution and compliance queries
- ☑ Direct users to relevant resources and guidance materials

## HIA Implementation Guide

*For the latest updates on HIA-related matters, please refer to HIA Implementation Guide*

HIA Implementation Guide for Healthcare Providers

Watch out for our emails to guide you on the onboarding process.

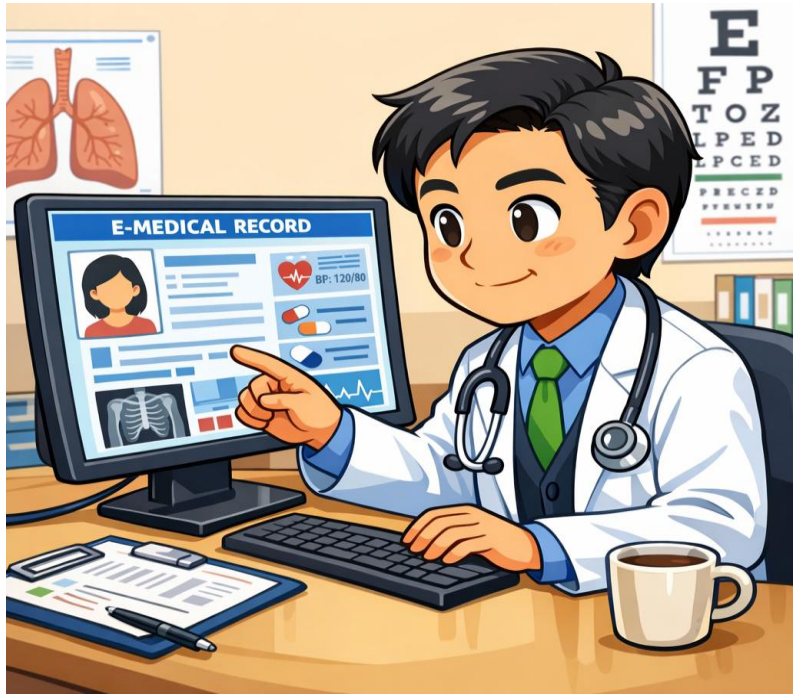
MINISTRY OF HEALTH
SINGAPORE

# Cybersecurity and Data Security (CS/DS) Measures under the Health Information Act (HIA)

Version as at 25 Sep 2026

An initiative of FORWARD SG

# (1) Safeguarding health information under HIA – what every healthcare staff must know




A. **Safeguard patient trust** through robust security measures and ensure patients feel safe when entrusting their health information to you for medical care.
   - Patients may feel embarrassed or have anxiety about their health information or concerns over how their medical conditions may affect their school, job prospects.

B. **Secure your digital foundation** when you implement cybersecurity and data security measures and defend against system compromises and breaches.

C. Every time you access a patient's medical record, order a lab test, write a prescription, you will handle and manage health information.

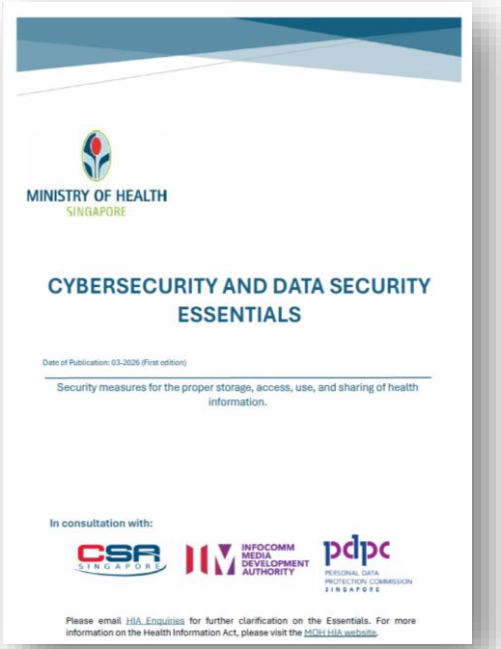
D. A careless email, an unlocked screen, or a lost USB drive can expose health information and cause real harm to the patients you care for.

# (2) Resources to help you understand and comply with the HIA

MOH issued a series of "self-help" resources in 2026 to assist HIA entities in implementing the relevant security measures to protect health information.

## A. CS/DS Essentials (March 2026)

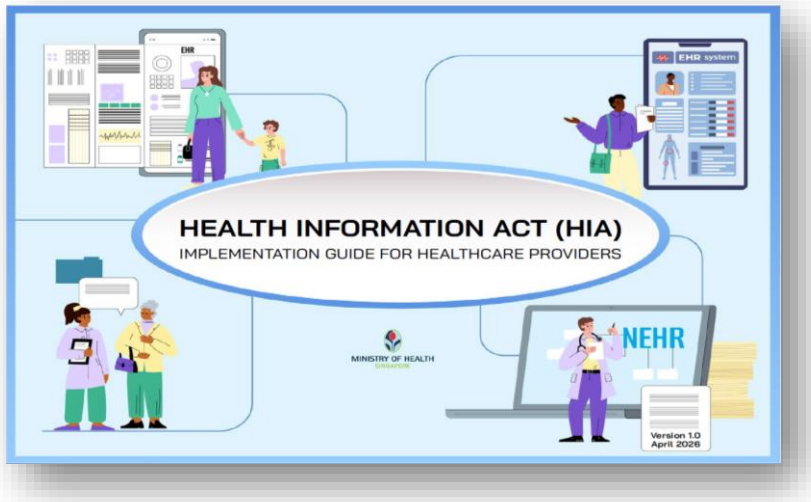
*"What are the Policies and Practices?"*




- Mandatory security measures for processing and managing health information.
- Replaced 2023 CS/DS Guidelines.

## B. Implementation Guide (August 2026)

*"How to operationalise the Policies and Practices?"*




- Operational aspects of compliance -
  - Ch 1: What healthcare providers need to do and by when.
  - Ch 2: Steps for NEHR contribution and access, NEHR Connect Grant (NCG).
  - Ch 3: Technical steps on cybersecurity, sample policy clauses, business continuity and incident response considerations.

# Part A: Overview of Cybersecurity and Data Security Measures

“What are the Policies and Practices?”

# (3) Overview of cybersecurity and data security measures covered today

- **Cybersecurity** focuses on protecting **all the digital information, computer systems, IT and software** your clinic uses every day and to keep them safe from attacks.
- **Data security** means protecting **all the health information** that you collect, store, use, and to safely dispose the information if no longer needed, determining who can access the health information.

**We will explain how to implement some of these security measures in the next section!**

| Section A: Cybersecurity (IT and device measures) | Section B: Data Security (Data practices) | Section C: Common practices (Organisation-wide) |
|---|---|---|
| 1. Install updates promptly | 1. Identify and protect health information | 1. Annual security training |
| 2. Anti-malware and firewalls | 2. Copy health information safely | 2. Vendors and cloud provider awareness |
| 3. Use a strong password, 2FA | 3. Transfer health information safely | 3. Audit and review |
| 4. Data back-up | 4. Control access to health information | 4. Dispose data safely |
| 5. Manage devices and assets | | 5. Business continuity and incident management |

# (4) Section A (Cybersecurity): Keep devices up to date and protected




## 1 Install updates promptly

**When your organisation's computer shows a software update prompt.**

☑ Prioritise critical updates.
☑ Consult IT support if updates keep failing.
☑ Be prompt in restarts after updates.




## 2 Anti-malware and firewalls

**Your organisation's computer should always have anti-virus running, it is intended to detect malicious software.**

☑ Enable anti-malware and conduct regular malware scans.
☑ Activate firewall to allow only authorised traffic.
☑ Plug in only authorised USB drives that are known to you.

# (4) Section A (Cybersecurity): Passwords, accounts, locking your screen

## 3 (A) Use strong passwords

**Having a strong password means having a good lock on the document.**

☑ At least 12 characters, mixed upper/lower case, numbers and symbols, e.g. Sun$hines4All

☑ Never use “password123” or your name.

## (B) Enable 2FA for key systems

**Two-factor authentication (2FA) is like having a second lock on your door.**

☑ Required for all admin and remote access to clinical systems.

## (C) Lock your screen when away

**Always lock your computer when you step away from your work desk, even for a minute.**

☑ Shortcut: Windows+L (PC) or Ctrl+Cmd+Q (Mac).

## (D) Never share your account

**Your login credentials are personal. Sharing accounts makes it impossible to trace who accessed patient records.**












# (4) Section A (Cybersecurity): Managing data, devices and assets




## 4 Data back-up

**Your organisation/IT team manages backups, you play a role too.**

☑ Perform backups regularly.
☑ Restrict backups to authorised personnel only.
☑ Report if clinical systems become unavailable unexpectedly.




## 5 Manage devices and assets

**Only use approved devices and software for clinical work.**

☑ Use only organisation-issued or approved devices to access patient records.
☑ Only install approved applications on organisation's computers.
☑ Avoid using "end-of-support" hardware or software assets.

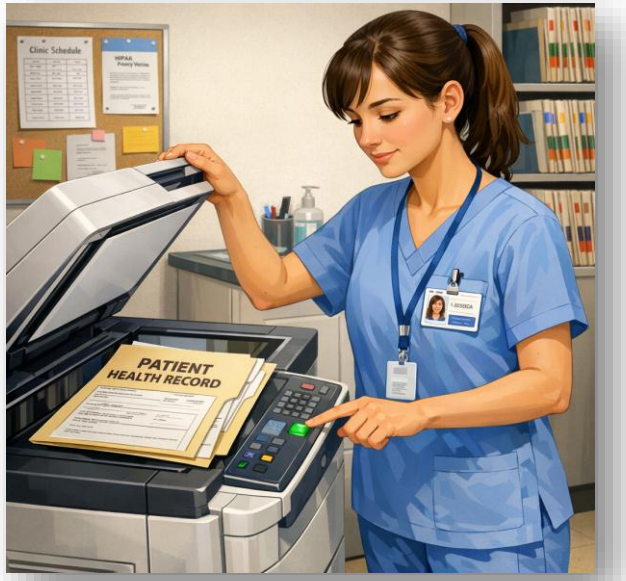
# (5) Section B (Data Security): Secure health information




## 1 Identify and secure health information

**Establish policies and processes to identify and secure health information.**

- ☑ Use a cable lock to secure equipment or devices and do not leave them unattended.
- ☑ Keep a clean desk policy by not leaving any health records unattended (i.e. they have to be within sight) when people move around your organisation.
- ☑ Limit access to hard copy records (on a need-to-know basis) and store them in locked cabinets in your organisation after use.
- ☑ Only retain health information if there is a business or legal purpose to do so.




## 2 Copy health information securely

**Establish policies and processes on making copies of health information.**

- ☑ Only make copies on a need-to-know basis by authorised parties and for official work purposes.
- ☑ Maintain possession of all copies made (e.g. collect print-outs quickly).
- ☑ Keep health records in your possession at all times when outside the organisation.

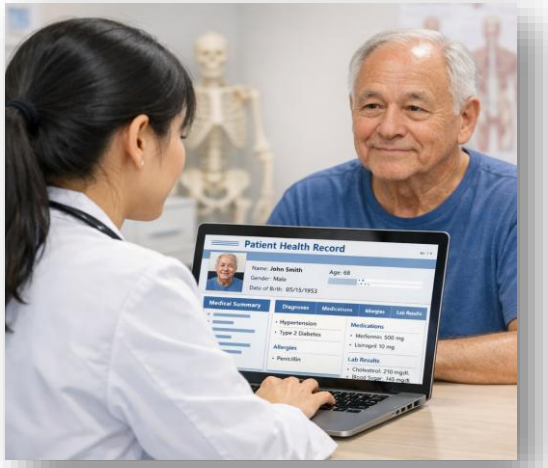
# (5) Section B (Data Security): Secure health information



## 3 Transfer health information securely

**Establish policies and processes for transferring health information safely**

- ☑ Encrypt the file / PDF before emailing and password protect the document.
- ☑ Send the password via a different channel (e.g. SMS or phone), not in the same email.
- ☑ Check recipient's email address before sending.
- ☑ Protect health information from accidental exposure (e.g. use privacy filter).




## 4 Control access to health information

**Establish policies and processes restricting access to health information.**

- ☑ The patient must be under your direct care.
- ☑ You have a legitimate need to know to carry out official job functions.
- ☑ You / your staff have been informed or made aware/acknowledge the data protection and security measures under law, corporate policies, and/or professional ethics/standards.

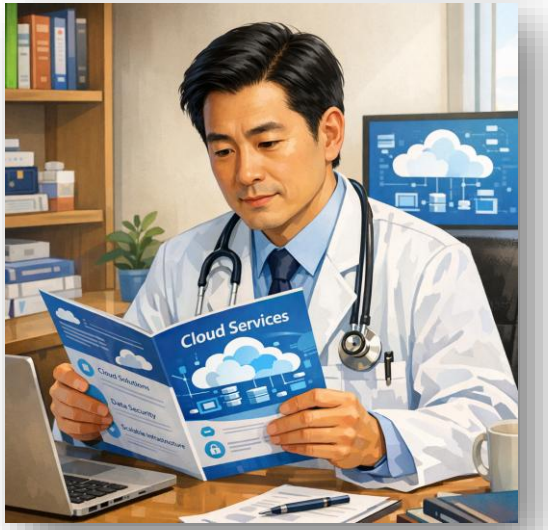
# (6) Section C (Common Practices): Training staff and managing vendors




## 1 Annual security training

**Staff should train at least once a year (whether in-house or external providers).**

- ☑ Topics may include how to spot phishing emails, safe handling of patient records, data protection and security, what to do if you suspect a breach.
- ☑ Staff can adopt cybersecurity, data security hygiene policies and processes in daily ops as this helps to ensure familiarity with security practices and expected behaviours.




## 2 Vendor and cloud provider awareness

**Be aware of the external systems that your organisation uses (e.g. CMS, telehealth portal, cloud storage).**

- ☑ Only use systems approved by your organisation.
- ☑ Health information should only be stored in IT-approved third-party tools.
- ☑ For cloud tools (e.g. shared drives), check with IT if you are uncertain.
- ☑ When in doubt, ask IT before using a new digital tool.

# (6) Section C (Common Practices): Review, disposal and continuity



## 3 Audit and review

**Review implementation of cybersecurity and data security safeguards for health information.**

- ☑ Your organisation should review security measures (e.g. at least annually).
- ☑ Conduct/cooperate with internal audits.
- ☑ Report any gaps noticed (e.g. alert organisation HQ).




## 4 Dispose data safely

**Reduce risk of unauthorised access through proper disposal of devices and data.**

- ☑ Paper records: use cross-cut shredder.
- ☑ Print-outs of health information should be disposed in designated bins.
- ☑ You should report misplaced or lost health information to IT.




## 5 (A) Business continuity

**Ensure organisational resilience through business continuity planning.**

- ☑ Know the manual backup process if systems go down.
- ☑ Know who to call for system downtime: have your IT helpdesk number recorded.
- ☑ Continue patient care safely using paper health records as fall-back if needed.

# (6) Section C (Common Practices): Review, disposal and continuity




## 5 (B) Incident management

**Establish up-to-date incident response plan on how to respond, manage and mitigate impact of cybersecurity incidents or data breaches.**

- ☑ Clear roles and responsibilities of staff involved in incident response process.
- ☑ Procedures to detect, respond, recover from threat scenarios.
- ☑ Comms plan and escalation, reporting to stakeholders.

**If you suspect a cyberattack or data breach - take these steps immediately!**

**(1) Stop and do not panic**
Do not try and fix it yourself. Stop all work on the affected systems.

**(2) Report to IT / manager / DPO**
Call your IT helpdesk or notify your manager / DPO immediately. Do not wait.

**(3) Preserve evidence**
Do not delete files, emails or logs. Leave the system as-is for IT / DPO to investigate.

**(4) Document what happened**
Write down what you saw, when/how it happened and any actions you took.

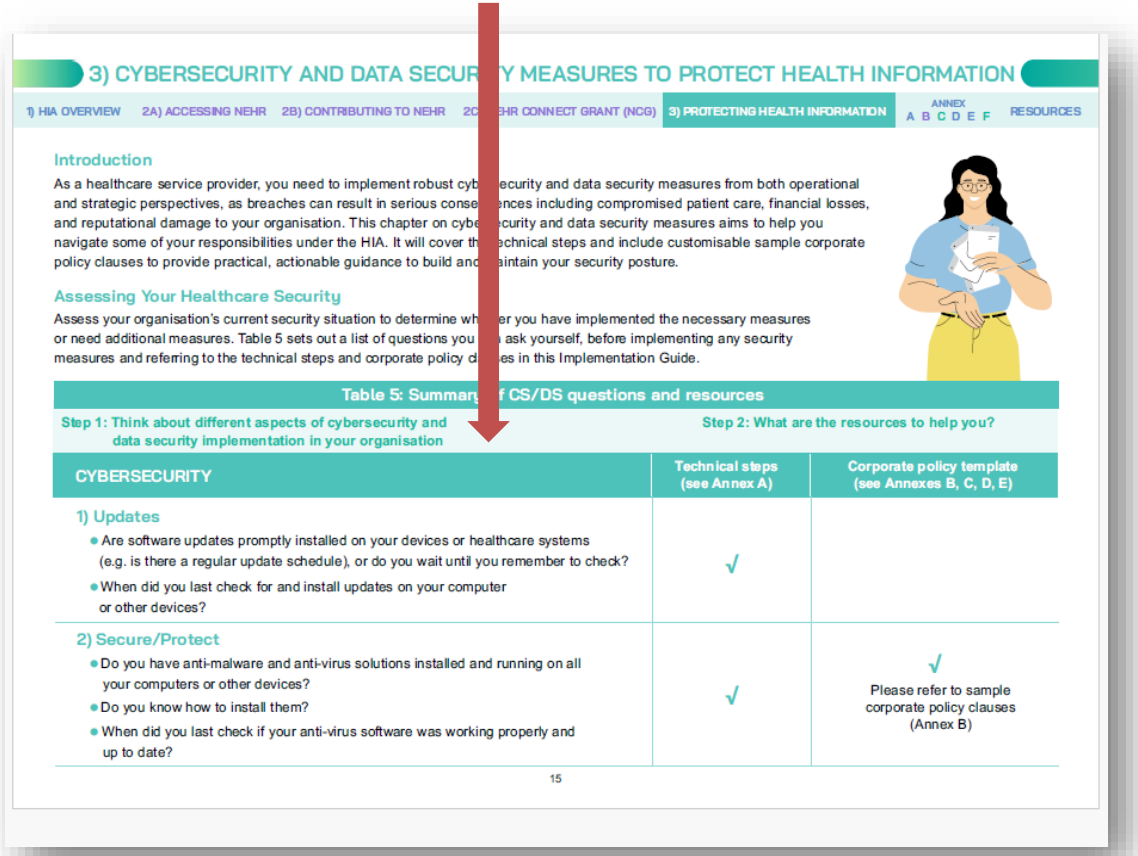
# Part B: Overview of Cybersecurity and Data Security (CS/DS) in the Implementation Guide

"How to operationalise the Policies and Practices?"

# (7A) Navigating the Implementation Guide CS/DS Section

A. The Cybersecurity and Data Security (CS/DS) sections within the Implementation Guide are premised on the CS/DS Essentials; and focus on how to operationalise the security requirements.

## Step 1: Think about different aspects of CS/DS implementation in your organisation



3) CYBERSECURITY AND DATA SECURITY MEASURES TO PROTECT HEALTH INFORMATION

1) HIA OVERVIEW | 2A) ACCESSING NEHR | 2B) CONTRIBUTING TO NEHR | 2C) NEHR CONNECT GRANT (NCG) | 3) PROTECTING HEALTH INFORMATION | ANNEX A B C D E F | RESOURCES

**Introduction**

As a healthcare service provider, you need to implement robust cybersecurity and data security measures from both operational and strategic perspectives, as breaches can result in serious consequences including compromised patient care, financial losses, and reputational damage to your organisation. This chapter on cybersecurity and data security measures aims to help you navigate some of your responsibilities under the HIA. It will cover the technical steps and include customisable sample corporate policy clauses to provide practical, actionable guidance to build and maintain your security posture.

**Assessing Your Healthcare Security**

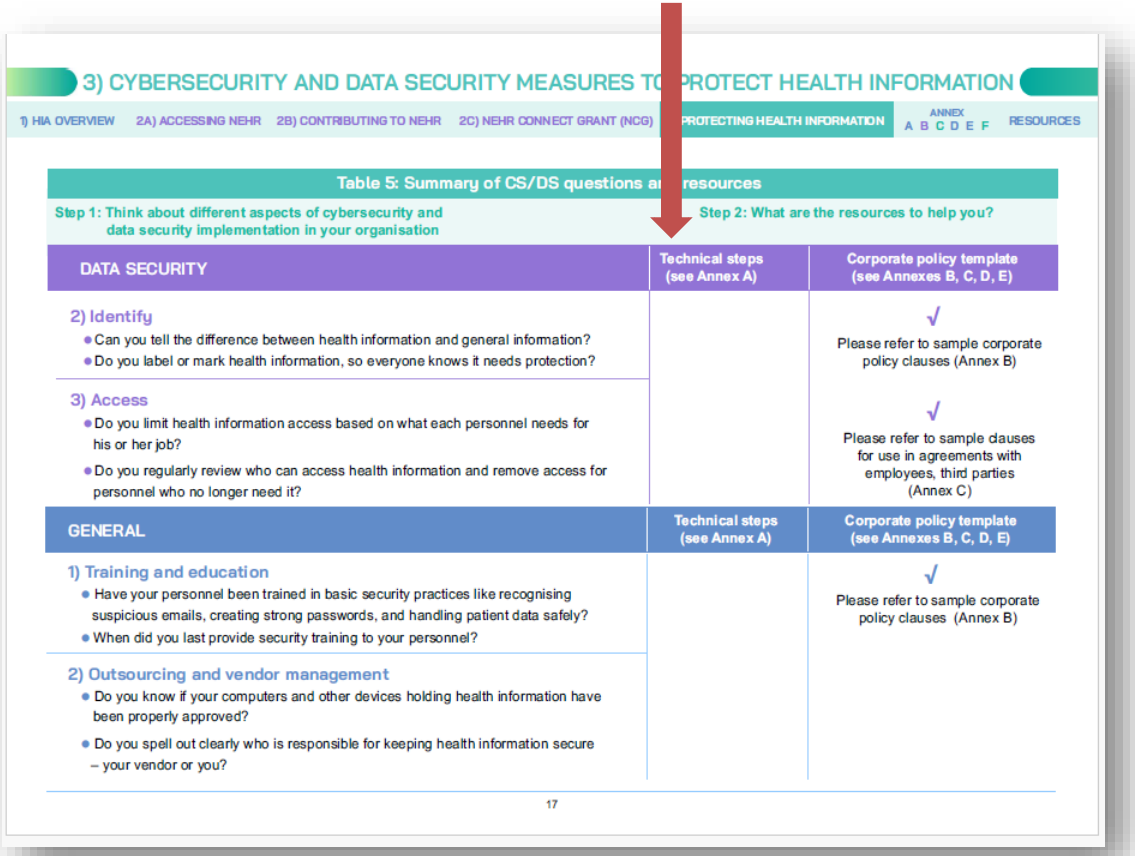
Assess your organisation's current security situation to determine whether you have implemented the necessary measures or need additional measures. Table 5 sets out a list of questions you can ask yourself, before implementing any security measures and referring to the technical steps and corporate policy clauses in this Implementation Guide.

**Table 5: Summary of CS/DS questions and resources**

| Step 1: Think about different aspects of cybersecurity and data security implementation in your organisation | Step 2: What are the resources to help you? | |
|---|---|---|
| **CYBERSECURITY** | **Technical steps (see Annex A)** | **Corporate policy template (see Annexes B, C, D, E)** |
| 1) Updates<br>• Are software updates promptly installed on your devices or healthcare systems (e.g. is there a regular update schedule), or do you wait until you remember to check?<br>• When did you last check for and install updates on your computer or other devices? | √ | |
| 2) Secure/Protect<br>• Do you have anti-malware and anti-virus solutions installed and running on all your computers or other devices?<br>• Do you know how to install them?<br>• When did you last check if your anti-virus software was working properly and up to date? | √ | √ Please refer to sample corporate policy clauses (Annex B) |

15

## Step 2: What are the measures to help you? (Refer to Annexes for the resources and templates)



3) CYBERSECURITY AND DATA SECURITY MEASURES TO PROTECT HEALTH INFORMATION

1) HIA OVERVIEW | 2A) ACCESSING NEHR | 2B) CONTRIBUTING TO NEHR | 2C) NEHR CONNECT GRANT (NCG) | 3) PROTECTING HEALTH INFORMATION | ANNEX A B C D E F | RESOURCES

**Table 5: Summary of CS/DS questions and resources**

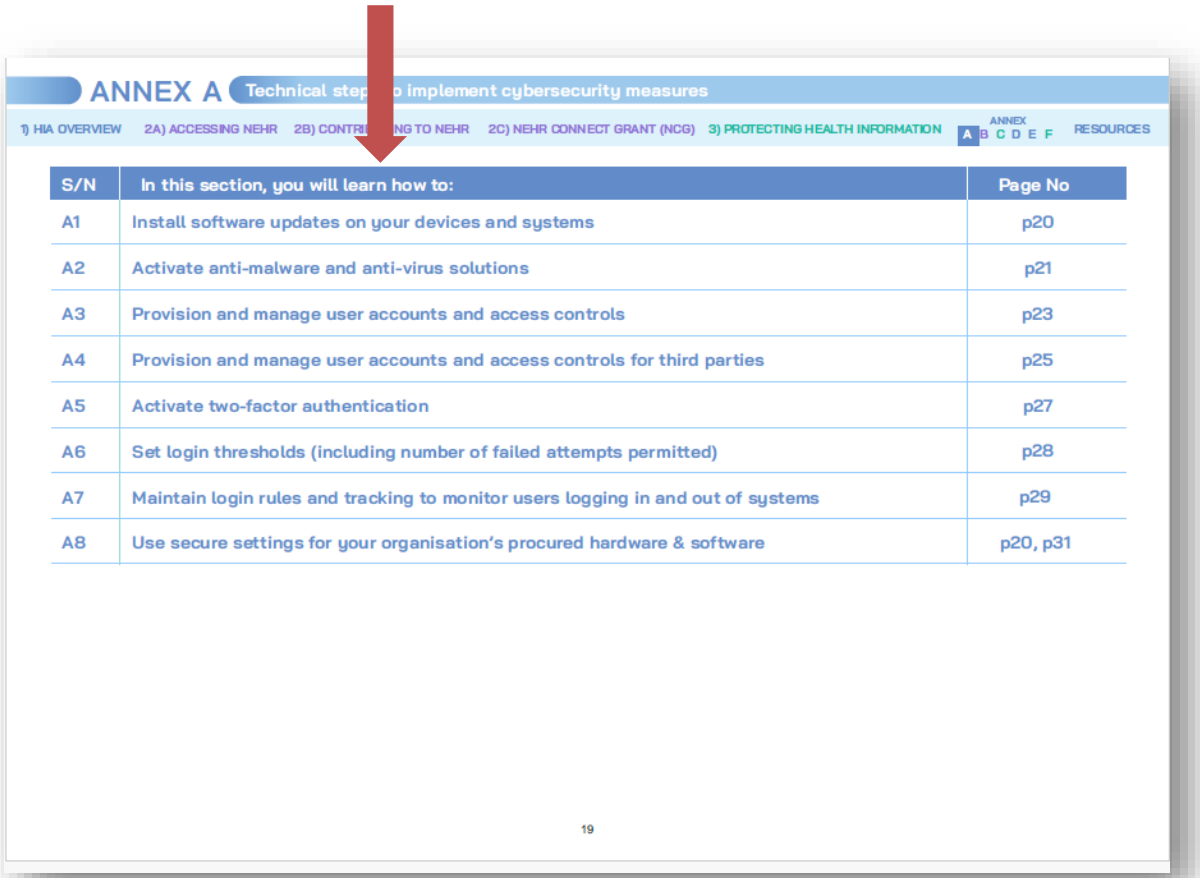
| Step 1: Think about different aspects of cybersecurity and data security implementation in your organisation | Step 2: What are the resources to help you? | |
|---|---|---|
| **DATA SECURITY** | **Technical steps (see Annex A)** | **Corporate policy template (see Annexes B, C, D, E)** |
| 2) Identify<br>• Can you tell the difference between health information and general information?<br>• Do you label or mark health information, so everyone knows it needs protection? | | √ Please refer to sample corporate policy clauses (Annex B) |
| 3) Access<br>• Do you limit health information access based on what each personnel needs for his or her job?<br>• Do you regularly review who can access health information and remove access for personnel who no longer need it? | | √ Please refer to sample clauses for use in agreements with employees, third parties (Annex C) |
| **GENERAL** | **Technical steps (see Annex A)** | **Corporate policy template (see Annexes B, C, D, E)** |
| 1) Training and education<br>• Have your personnel been trained in basic security practices like recognising suspicious emails, creating strong passwords, and handling patient data safely?<br>• When did you last provide security training to your personnel? | | √ Please refer to sample corporate policy clauses (Annex B) |
| 2) Outsourcing and vendor management<br>• Do you know if your computers and other devices holding health information have been properly approved?<br>• Do you spell out clearly who is responsible for keeping health information secure – your vendor or you? | | |

17

# (7B) Navigating the Implementation Guide CS/DS Section – Summary Table

A. We have provided a table of contents to help you find the resources / templates that you need.

**The Technical Steps on Cybersecurity are based on the CS/DS Essentials**



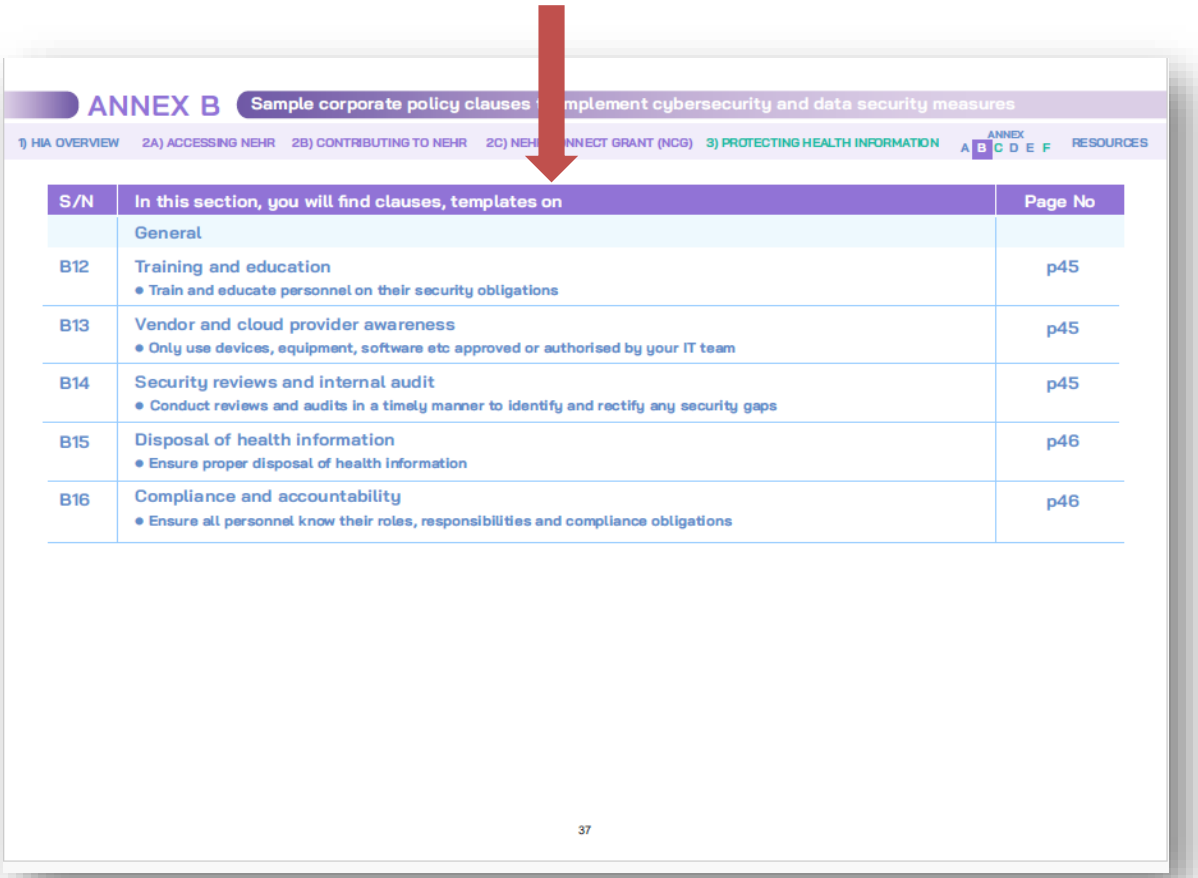
ANNEX A Technical steps to implement cybersecurity measures

1) HIA OVERVIEW | 2A) ACCESSING NEHR | 2B) CONTRIBUTING TO NEHR | 2C) NEHR CONNECT GRANT (NCG) | 3) PROTECTING HEALTH INFORMATION | ANNEX A B C D E F | RESOURCES

| S/N | In this section, you will learn how to: | Page No |
|---|---|---|
| A1 | Install software updates on your devices and systems | p20 |
| A2 | Activate anti-malware and anti-virus solutions | p21 |
| A3 | Provision and manage user accounts and access controls | p23 |
| A4 | Provision and manage user accounts and access controls for third parties | p25 |
| A5 | Activate two-factor authentication | p27 |
| A6 | Set login thresholds (including number of failed attempts permitted) | p28 |
| A7 | Maintain login rules and tracking to monitor users logging in and out of systems | p29 |
| A8 | Use secure settings for your organisation's procured hardware & software | p20, p31 |

19

**The sample corporate policy clauses are developed based on the CS/DS Essentials**



ANNEX B Sample corporate policy clauses to implement cybersecurity and data security measures

1) HIA OVERVIEW | 2A) ACCESSING NEHR | 2B) CONTRIBUTING TO NEHR | 2C) NEHR CONNECT GRANT (NCG) | 3) PROTECTING HEALTH INFORMATION | ANNEX A B C D E F | RESOURCES

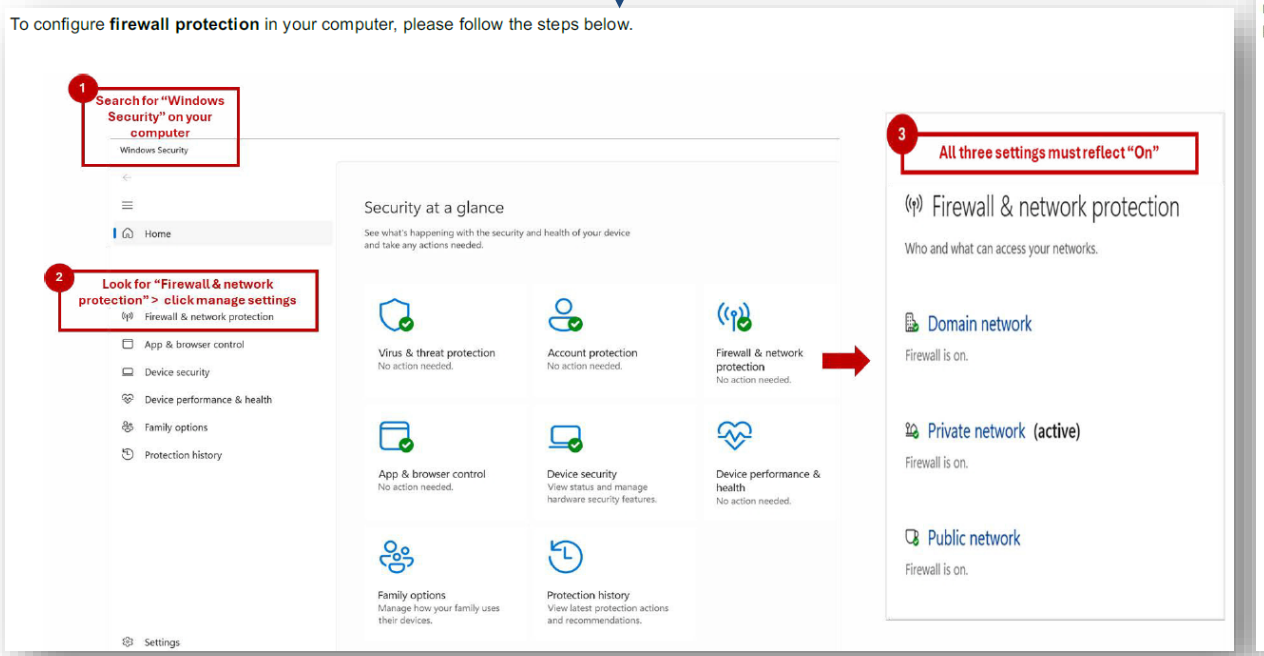
| S/N | In this section, you will find clauses, templates on | Page No |
|---|---|---|
| | General | |
| B12 | Training and education<br>• Train and educate personnel on their security obligations | p45 |
| B13 | Vendor and cloud provider awareness<br>• Only use devices, equipment, software etc approved or authorised by your IT team | p45 |
| B14 | Security reviews and internal audit<br>• Conduct reviews and audits in a timely manner to identify and rectify any security gaps | p45 |
| B15 | Disposal of health information<br>• Ensure proper disposal of health information | p46 |
| B16 | Compliance and accountability<br>• Ensure all personnel know their roles, responsibilities and compliance obligations | p46 |

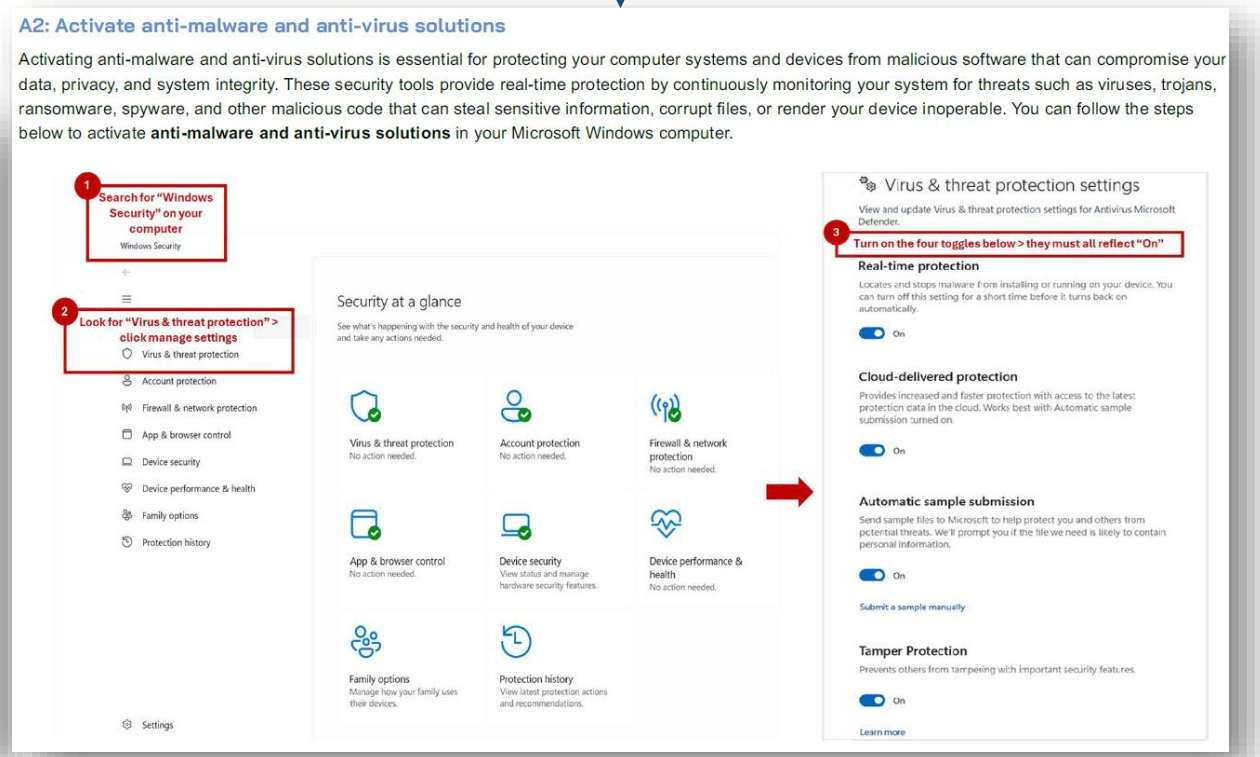
37

# (8) Technical steps to implement cybersecurity measures

A. These technical steps are based on the Windows Operating System and are intended to serve as a general reference. Given that computing environments may differ across organisations, we recommend adapting these steps to align with your organisation's specific systems prior to implementation.

**(I) Screen-by-screen guide on security configuration settings.**

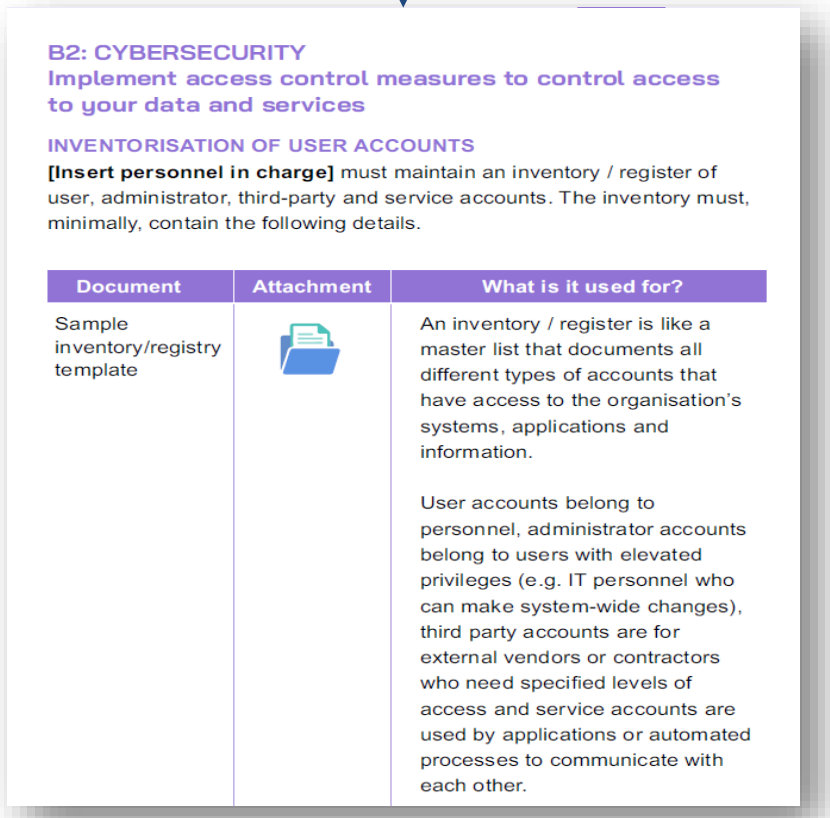


# (9) Sample corporate policy clauses on cybersecurity and data security measures

A. These sample corporate policy clauses serve as a general reference for organisations to refer to in reviewing your internal policies and practices to implement the cybersecurity and data security measures.

**(I) Clearly marked headers to indicate key security measures**



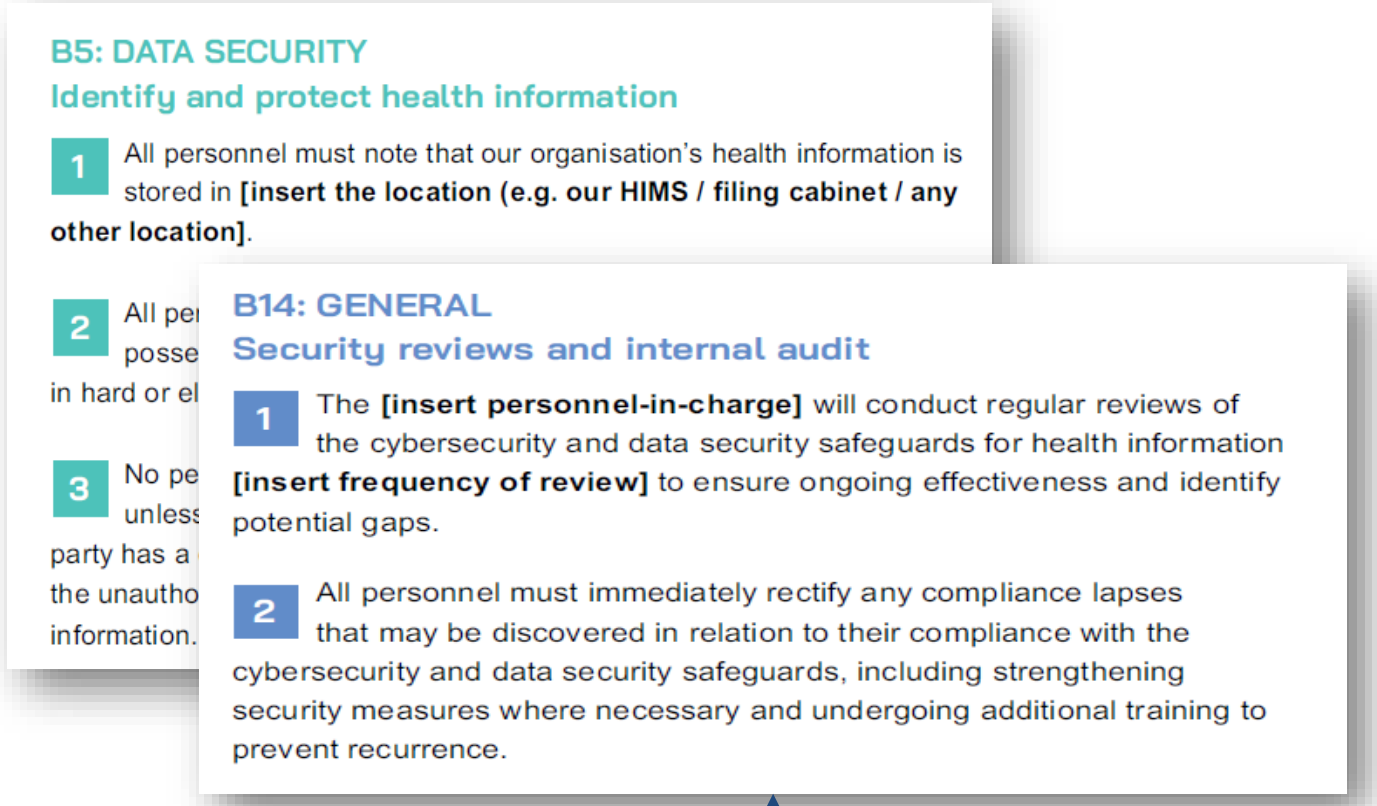
B2: CYBERSECURITY

Implement access control measures to control access to your data and services

INVENTORISATION OF USER ACCOUNTS

**[Insert personnel in charge]** must maintain an inventory / register of user, administrator, third-party and service accounts. The inventory must, minimally, contain the following details.

| Document | Attachment | What is it used for? |
|---|---|---|
| Sample inventory/registry template | | An inventory / register is like a master list that documents all different types of accounts that have access to the organisation's systems, applications and information.<br><br>User accounts belong to personnel, administrator accounts belong to users with elevated privileges (e.g. IT personnel who can make system-wide changes), third party accounts are for external vendors or contractors who need specified levels of access and service accounts are used by applications or automated processes to communicate with each other. |



B5: DATA SECURITY

Identify and protect health information

1 All personnel must note that our organisation's health information is stored in **[insert the location (e.g. our HIMS / filing cabinet / any other location]**.

2 All pe
posse
in hard or el

3 No pe
unless
party has a
the unautho
information.

B14: GENERAL

Security reviews and internal audit

1 The **[insert personnel-in-charge]** will conduct regular reviews of the cybersecurity and data security safeguards for health information **[insert frequency of review]** to ensure ongoing effectiveness and identify potential gaps.

2 All personnel must immediately rectify any compliance lapses that may be discovered in relation to their compliance with the cybersecurity and data security safeguards, including strengthening security measures where necessary and undergoing additional training to prevent recurrence.

**(II) Clearly marked areas that require contextualisation**

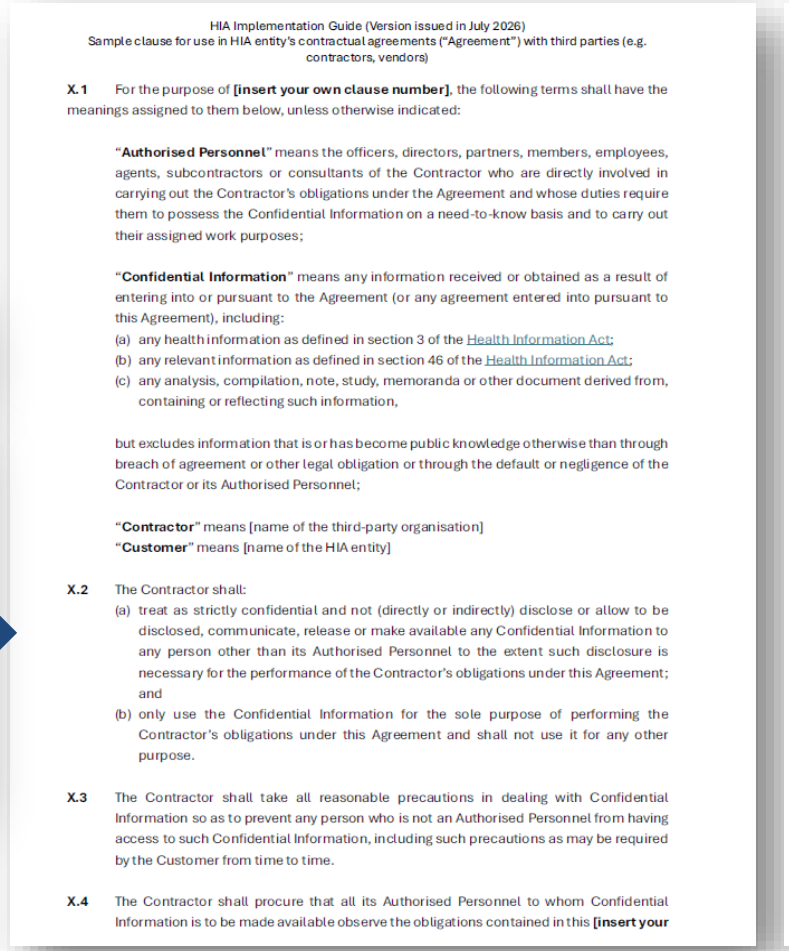
# (10) Sample data disclosure and confidentiality clauses for third-parties and employees

A. These sample clauses can be referred to in reviewing your contracts with your third parties and employees, to require them to protect health information.

**(I) Clearly marked headers and tables to find samples**

Notes and instructions for use of sample data disclosure and confidentiality clauses

| Document | Attachment |
|---|---|
| Sample clause for use in HIA entity's contractual agreements with third parties (e.g. contractors, vendors) | |
| Sample clause for use in HIA entity's employment agreements | |



HIA Implementation Guide (Version issued in July 2026)
Sample clause for use in HIA entity's contractual agreements ("Agreement") with third parties (e.g. contractors, vendors)

**X.1** For the purpose of **[insert your own clause number]**, the following terms shall have the meanings assigned to them below, unless otherwise indicated:

"**Authorised Personnel**" means the officers, directors, partners, members, employees, agents, subcontractors or consultants of the Contractor who are directly involved in carrying out the Contractor's obligations under the Agreement and whose duties require them to possess the Confidential Information on a need-to-know basis and to carry out their assigned work purposes;

"**Confidential Information**" means any information received or obtained as a result of entering into or pursuant to the Agreement (or any agreement entered into pursuant to this Agreement), including:
(a) any health information as defined in section 3 of the Health Information Act;
(b) any relevant information as defined in section 46 of the Health Information Act;
(c) any analysis, compilation, note, study, memoranda or other document derived from, containing or reflecting such information,

but excludes information that is or has become public knowledge otherwise than through breach of agreement or other legal obligation or through the default or negligence of the Contractor or its Authorised Personnel;

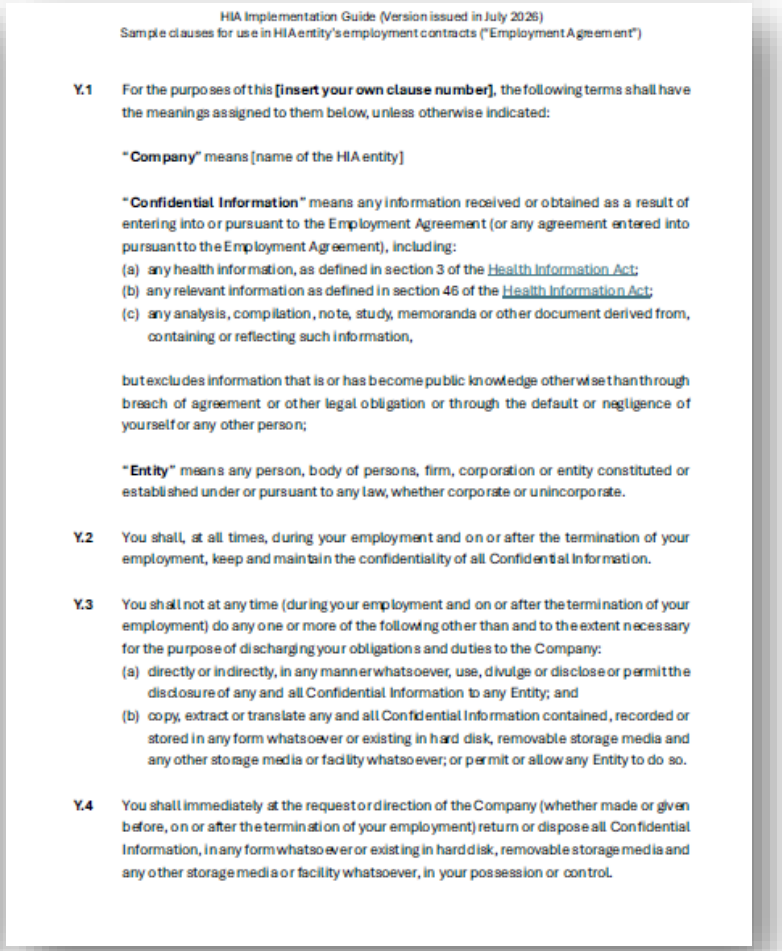
"**Contractor**" means [name of the third-party organisation]
"**Customer**" means [name of the HIA entity]

**X.2** The Contractor shall:
(a) treat as strictly confidential and not (directly or indirectly) disclose or allow to be disclosed, communicate, release or make available any Confidential Information to any person other than its Authorised Personnel to the extent such disclosure is necessary for the performance of the Contractor's obligations under this Agreement; and
(b) only use the Confidential Information for the sole purpose of performing the Contractor's obligations under this Agreement and shall not use it for any other purpose.

**X.3** The Contractor shall take all reasonable precautions in dealing with Confidential Information so as to prevent any person who is not an Authorised Personnel from having access to such Confidential Information, including such precautions as may be required by the Customer from time to time.

**X.4** The Contractor shall procure that all its Authorised Personnel to whom Confidential Information is to be made available observe the obligations contained in this **[insert your**

Data disclosure and confidentiality clauses for third-parties



HIA Implementation Guide (Version issued in July 2026)
Sample clauses for use in HIA entity's employment contracts ("Employment Agreement")

**Y.1** For the purposes of this **[insert your own clause number]**, the following terms shall have the meanings assigned to them below, unless otherwise indicated:

"**Company**" means [name of the HIA entity]

"**Confidential Information**" means any information received or obtained as a result of entering into or pursuant to the Employment Agreement (or any agreement entered into pursuant to the Employment Agreement), including:
(a) any health information, as defined in section 3 of the Health Information Act;
(b) any relevant information as defined in section 46 of the Health Information Act;
(c) any analysis, compilation, note, study, memoranda or other document derived from, containing or reflecting such information,

but excludes information that is or has become public knowledge otherwise than through breach of agreement or other legal obligation or through the default or negligence of yourself or any other person;

"**Entity**" means any person, body of persons, firm, corporation or entity constituted or established under or pursuant to any law, whether corporate or unincorporate.

**Y.2** You shall, at all times, during your employment and on or after the termination of your employment, keep and maintain the confidentiality of all Confidential Information.

**Y.3** You shall not at any time (during your employment and on or after the termination of your employment) do any one or more of the following other than and to the extent necessary for the purpose of discharging your obligations and duties to the Company:
(a) directly or indirectly, in any manner whatsoever, use, divulge or disclose or permit the disclosure of any and all Confidential Information to any Entity; and
(b) copy, extract or translate any and all Confidential Information contained, recorded or stored in any form whatsoever or existing in hard disk, removable storage media and any other storage media or facility whatsoever; or permit or allow any Entity to do so.

**Y.4** You shall immediately at the request or direction of the Company (whether made or given before, on or after the termination of your employment) return or dispose all Confidential Information, in any form whatsoever or existing in hard disk, removable storage media and any other storage media or facility whatsoever, in your possession or control.

Data disclosure and confidentiality clauses for employees

# (11) Considerations for formulating a Business Continuity Plan (BCP)

A. A Business Continuity Plan (BCP) is a documented strategy that helps organisations maintain essential services and critical operations during disruptions such as cyberattacks or data breaches. When developing a BCP, organisations should consider their specific operating context and risk profile to identify gaps and inform the plan's scope and design.

B. A printed copy should also be kept on-site for reference when systems are unavailable.

## (I) Clearly marked key areas to consider in a BCP

### D1: Critical functions and service continuity

1 Understand which functions your organisation cannot afford to stop, even during a cyberattack or data breach.

2 Consider whether your consultation rooms can operate independently of your Health Information Management System (HIMS) and other systems (e.g. when national claims systems are

### D2: Paper-based backup readiness

1 Depending on the extent and severity of the cyberattack, your digital systems may be rendered completely inaccessible for hours or days. Assess how prepared your organisation is to revert to paper-based operations at short notice ("safe mode clinic operations").

(a) Consider whether you have paper templates for consultations, appointments, and billing.

(b) Think about whether these paper templates are physically accessible in the right locations (e.g. consultation rooms, reception, dispensary) and whether personnel know where to find them.

(c) Assess how your organisation would handle the transition back to digital systems after restoration, including how to update your HIMS based on the paper records.

## (II) Sample questions to ask relevant parties

Table 7: Sample questions to ask your CMS provider/IT vendor

| Key categories of questions | Sample questions to ask your CMS provider / IT vendor |
|---|---|
| Understanding what gets backed up | • What data in our organisation's system is backed up — does this include all patient records, appointment histories, clinical notes?<br>• Is there any data that is not covered by your backup process that we should be aware of? |
| Frequency and timing | • How often are backups performed — is it daily, hourly, or in real time?<br>• At what time of day do backups occur, and does this affect system performance during clinic hours? |
| Storage and location | • Where are our organisation's backups stored — is it on the same server as our live data, or in a separate and secure location?<br>• Are backups stored in Singapore, and if outside of Singapore, which country and under what data protection arrangements? |
| Recovery | • If our organisation experiences data loss or a ransomware attack, how quickly can you restore our data, and what is the process for requesting a recovery?<br>• What is the oldest point in time our organisation can recover data from — for example, can we go back 7 days, 30 days, or longer? |

## (III) Sample response card to address cyberattack

Table 8: Example of a response card for ransomware

**Ransomware Response Card**

How to spot - does something look wrong, please check for these signs?

- Files cannot be opened or have strange names
- A ransom message has appeared on screen

What to do - If any of the above is happening, please follow these steps promptly.

1) DISCONNECT
- Unplug the network cable or turn off Wi-Fi on affected computers.
- Do not switch the computer off completely to retain forensic data for investigation.

2) STOP AND ASSESS

Can your organisation still see patients safely?
- If yes, If yes, consider activating your BCP (e.g. switch to paper records).
- If no, consider diverting patients and to inform them promptly, or reschedule appointments.

3) CALL FOR HELP

Keep names and numbers of parties to call.
- CMS provider / IT vendor
- Key personnel in your organisation (e.g. clinic manager)

4) DO NOT PAY THE RANSOM
- Paying does not guarantee recovery.
- Please consult and wait for advice from your IT vendor first.

5) REPORT IF PATIENT DATA IS AFFECTED
- Have the reporting hotline numbers of the relevant authorities ready.

6) WAIT FOR THE "ALL CLEAR"
- Only restart and restore systems once your IT vendor confirms it is safe to do so.
- Change all passwords after restoration.

After the Incident:
- Write down what happened and when.
- Your organisaton will need this for reporting and to prevent it from happening again.

Prepared by: _____ | Version: _____ | Date: _____

# (12) Considerations for formulating an Incident Response Plan (IRP)

A. An incident response plan (IRP) provides staff with a clear, step-by-step guide on what to do, who to contact, and how to keep patients safe in the critical first moments of a cyberattack or data breach. A good IRP does not need to be technical or complex — it simply needs to be practical, easy to follow under pressure, and tailored to how your organisation operates.

B. A printed copy should be kept on-site for quick reference when systems are unavailable.

## (I) Clearly marked key areas to consider in an IRP

### E1: Scope

When developing or reviewing your Incident Response Plan (IRP), you should consider the following areas.

**1 INCIDENT RESPONSE TEAM**

- Clearly define who falls within its scope, having considered your organisation size, personnel strength etc.
- Determine whether it covers not just full-time employees, but also part-time / temp staff, locum doctors. It is important to ensure that all personnel who come into contact with health information - regardless of their employment status - are aware of and bound by your IRP.
- Have a clear process for onboarding new staff to the IRP and for maintaining awareness and readiness across your team over time.

**2 SYSTEMS**

- Maintain a current and complete inventory of all systems used to process or store health information.
- Consider whether it covers personal devices such as mobile phones that may be used for work purposes, as these can often be overlooked.
- Assess whether older or legacy systems that may not be actively monitored are adequately covered, as these can present vulnerabilities that are easily missed.

## (I) Examples of incidents and spotting them

### E3: Types of incidents and how to spot them

In a busy clinic, the earliest warning signs of a cyberattack or data security incident can be easy to miss or dismiss. The sooner an incident is identified, the sooner you can contain it. **Table 10** contains a list of non-exhaustive but common situations where an incident may have occurred. If you observe any of these situations, treat it as a potential incident and immediately follow the response steps in **E4: Immediate response steps**.

**Table 10: Incident Examples**

**1 Cybersecurity attacks occur when malicious actors attempt to gain unauthorised access to computer systems or disrupt their operation.**

⚠ System locked or files cannot be opened (e.g. ransomware)

- Files have been renamed with unusual extensions (e.g. '.lockbit', '.wncry', '.conti').
- A message appears on screen demanding payment to unlock files.
- Patient records that were accessible previously can no longer be opened.
- Clinic management systems display errors when accessing patient data.

⚠ Suspicious system behaviour (e.g. malware/hacking)

- Emails sent from the clinic account without personnel doing so.
- Unexpected pop-up windows requesting passwords.
- New programmes or icons appearing that were not installed by personnel.
- Mouse cursor moving or actions occurring without user control.

## (III) How to respond to a cybersecurity incident or data security incident

### E4: Immediate response steps

When a cybersecurity incident or data breach is suspected, act quickly but calmly. When in doubt, treat suspected incidents as real incidents as it is better to take precautionary steps than to let a real incident worsen. If you have an IT or cybersecurity provider, engage them immediately and follow their guidance throughout these steps. If you do not have an existing provider, consider engaging a qualified vendor[12] immediately to assist with technical investigation, containment and recovery. The steps below provide basic guidance and they can be performed simultaneously, where appropriate **(see Table 11)**. However, complex incidents require expert assistance to fully resolve and prevent recurrence.

**Table 11: Response Steps**

| STEPS TO TAKE | RESPONDING TO A SUSPECTED CYBERSECURITY INCIDENT | RESPONDING TO A SUSPECTED DATA SECURITY INCIDENT |
|---|---|---|
| STEP 1: STOP AND DO NOT PANIC<br>Take immediate steps to prevent the situation from getting worse. When in doubt, act quickly to contain potential damage. | • Disconnect affected computer(s) from the internet immediately by unplugging the ethernet cable or turning off Wi-Fi.<br>• If multiple computers show similar problems, disconnect them as well.<br>• Do not restart affected computer(s) .<br>• Ask personnel to immediately stop using any system(s) showing problems. | • If an email was sent to the wrong recipient, attempt to recall the email immediately, if possible.<br>• Alternatively, contact the recipient and ask them to delete the email without opening attachments.<br>• If documents were disclosed accidentally, retrieve them immediately, if possible. |

- For any HIA-related feedback or enquiries, please write in to HIA-related feedback or enquiries

- For additional information and details, visit https://www.healthinfo.gov.sg

# Thank you