Health Information Act: What You Need to Know and Do

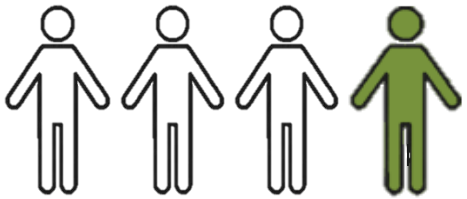
MINISTRY OF HEALTH
SINGAPORE

Overview of Health Information Act (HIA)

An initiative of
FORWARD SG

Current Healthcare Landscape

Singapore's Ageing Population



By 2030, 1 in 4 Singaporeans will be aged 65 and above

This is a significant demographic shift that brings a higher burden of chronic diseases and higher proportion of patients with multiple co-morbidities

Healthcare is shifting to the Community

Major programmes launched to manage health within communities: Healthier SG, Age Well SG

- *Healthcare delivery will increasingly extend beyond hospitals to the community, and cut across multiple settings*
- *Each transition = different providers, repeated assessments, fragmented information*
- *Need for coordinated care across hospitals, outpatient clinics and community health partners*
- *Gap: Key health information not accessible by healthcare providers when patients move across healthcare settings*

How does HIA aim to address this gap?

HIA's Goal: One Patient, One Health Summary, One Care Journey

Sharing of Key Health Information through NEHR

- Established in 2011, the National Electronic Health Record system (NEHR) is a centralised repository of key health information.
- Today, all public hospitals and polyclinics are already contributing to NEHR.
- Most GP clinics have also onboarded, with Healthier SG.
- Most private hospitals also onboarded, and the rest have committed to onboard within this year
- Hence, the bulk of key healthcare services are on NEHR, leaving a relatively small gap to plug among e.g. specialist clinics, laboratories and dental clinics.
- HIA will **close the last mile by requiring all licensed healthcare providers to contribute key health information to NEHR**

HIA: Sharing of Key Health Information through NEHR

Contribution of Key Health Information

- NEHR **consolidates key health information** from healthcare providers
- Singaporeans benefit from **enhanced quality of care, lower costs with reduced duplication, and better coordinated care**.

Benefits to Singapore Residents

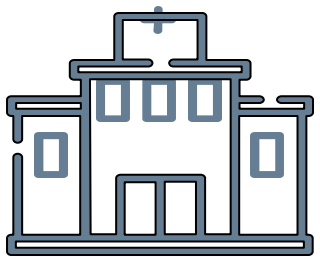
Better Care Quality:
Enables more effective care and reduces patient safety risks (e.g. inappropriate medication)

Lower Costs: Reduces duplicate investigations

Better Coordinated Care:
Across hospitals, clinics, and community healthcare partners

What does HIA mean to healthcare providers?

Ensuring timely and accurate contributions and protecting health information



Healthcare providers must:

Contribute

- Ensure the **accurate, timely and complete contribution** of key health information to NEHR

Protect and Appropriate Use

- Ensure a **secure connection** to NEHR and protect health information e.g. meet cyber and data security requirements
- Appoint authorised individuals who can access NEHR for care and regularly upkeep this list
- Not access NEHR for employment and insurance purposes
- Be aware that patients can monitor access to their NEHR records and place access restrictions
- Implement policies and practices to **ensure appropriate access, collection and disclosure of NEHR information** e.g. training for staff and audits

Report

- **Notify MOH of confirmed cybersecurity incidents and data breaches** in a timely manner

Phased Implementation according to Readiness of Providers

	Batch 1	Batch 2	Batch 3
Service Type	• Outpatient Medical Service (GP) • Acute Hospital • Community Hospital • Clinical Laboratory • Radiological Service • Nuclear Medicine Service	• Outpatient Medical Service (Specialist) • Nursing Home • Contingency Care Service • Outpatient Renal Dialysis	• Outpatient Dental Service • Ambulatory Surgical Centre • Assisted Reproduction • Retail Pharmacy
When healthcare providers can start accessing NEHR	• Healthcare providers with existing access can continue using NEHR. • Healthcare providers who wish to access can start applying for access now.		
Timeline to start contribution to NEHR, and implement cybersecurity and data security (CS/DS) measures	By September 2027	By September 2028	By March 2030

Note:

1. *For licensees providing multiple service types, NEHR contribution requirements apply according to each service's respective implementation timeline.*
2. *OMS clinics who have indicated to offer both "General Medical" and "Specialist Medical" services in Healthcare Application and Licensing Portal (HALP) will be covered under Batch 2 implementation for NEHR contribution (i.e. Sep 2028)*

Calibrated Actions for Non-Compliance to NEHR Contribution

NON-COMPLIANCE

1

MOH will **work with healthcare providers to resolve technical difficulties** (e.g. incompatible systems, system issues)

2

If necessary, MOH **may issue directions** to require the healthcare provider to take steps to remedy non-compliances or prevent recurrence

3

Should providers fail to respond to directions, HIA allows for:

- Letters of advice/warning
- Suspension of contribution or access to NEHR
- Composition of offences

4

For **deliberate or persistent non-compliance**, prosecution will be considered

Penalties in HIA are calibrated based on nature and impact of offence

Non-compliance with contribution requirements is **NOT** an offence in the first instance, as we understand that there may be genuine challenges with onboarding NEHR. For non-compliances, MOH will look at the facts of each case carefully.

Actions relating to Cybersecurity and Data Security Incidents

- Healthcare providers are strongly encouraged to adopt a HIA-Compliant HIMS as some of the cybersecurity requirements would have been built into the HIMS.
- However, healthcare providers will also need to put in place CS/DS requirements for other IT systems, including people and process aspects.
- MOH will provide guidance, resources and support to healthcare providers in implementing the CS/DS measures
- In the event of any data or cybersecurity incidents, the circumstances surrounding the incident are salient to determining liability.
- Actions will be taken if there is deliberate or reckless non-compliance to the CS/DS requirements.

MINISTRY OF HEALTH
SINGAPORE

NEHR Contribution Requirements

Healthier SG

An initiative of

FORWARD SG

The Aims of the NEHR

- Safer and more efficient care through:
  - Reduction in unnecessary duplicative tests.
  - Access to information in a timely manner (e.g. allergies)
  - More holistic view of patients' health conditions.

- Many of our patients are not familiar, or are not able to remember, all their health information.

- This information is made available to care providers to refer to **if** they deem necessary.

What needs to be contributed?

What needs to be contributed

Key health information depending on service provided for Singaporeans/PRs/FIN Holders only.

For example – medical clinics[1]:

a. Visit details (date/time, location)
b. Reason for visit/diagnosis
c. Allergies
d. Vaccinations given
e. Medications prescribed/dispensed
f. Referral letters
g. Surgical procedures[2]
h. Cardiac reports (ECGs)

What does NOT need to be contributed

1. Licensees are not expected to convert and contribute all historical data.
2. Licensees are not expected to contribute their detailed progress notes.
3. Laboratory/Radiology reports – these will be contributed by the Laboratories/ Radiology clinics.

[1] Other types of services will be required to submit other data types relevant to their service, e.g. inpatient facilities will be required to submit Discharge summaries, dental clinics will be required to submit Dental Notes – **Refer to ANNEX A (First Schedule)**

[2] These information types will be required at a later date.

Contribution Considerations

- Contributors should bear in mind that the information they submit will be used by other providers in the management of their patients.

- Contributors should ensure that the information contributed is complete and accurate.

Handling of errors:

- Where factual errors are detected (e.g. Left vs Right) they should be changed. However, clinicians are not required to change their professional opinions.

Health Information Management Systems

- **Health Information Management Systems (HIMS)** is an umbrella term that refers to IT systems used in the handling/management of healthcare information by healthcare providers.

- You may be more familiar with some of these terms:
  - Clinic Management Systems (CMSes)
  - Electronic Medical Records (EMR) or Electronic Health Records (EHRs)
  - Laboratory Information Systems (LISes)
  - Radiology Information Systems (RISes)

How to contribute?

- NEHR was designed to reduce the need for duplicative entry.
- Many licensees are already using IT systems to perform tasks that can automatically contribute to NEHR

  For example:

Features in Clinic Management System (CMS)	Data Types Required for contribution
Patient registration	a. Visit details
Printing Bills/Invoices	
Printing medication labels / Tracking inventory	b. Medications prescribed/dispensed
Submit claims	c. Reason for visit / diagnosis d. Vaccinations given
Capture allergies	e. Allergies

- HIA-Compliant HIMS will automatically submit data to NEHR as they are entered into the system

HIA-Compliant HIMS

3 Requirements:

1. Meet NEHR Connectivity requirements.
2. Have a **Cyber Essentials for HIMS Vendors** certification or equivalent.
3. Declared compliance with Data Portability practices.*

1. Ensure that data contributed is in the proper format and have the necessary requirements/components.
2. Ensure proper error and amendment handling.
3. Facilitate context-switching to NEHR.

* Applicable to commercial HIMS systems.

A list of commercial HIA-Compliant HIMS can be found online at: https://for.sg/hchlist

Alternatives for pen-and-paper clinics

- Adopting a HIMS is the recommended way for clinics who need to contribute to the NEHR.

- Special cases:
  - Clinics that need additional time to onboard a HIMS.
  - Other special scenarios.

- Alternative Contribution Channel (ACC): A web-based portal that will allow clinics to submit data to NEHR.
  - Provided as a temporary measure.
  - Will require manual effort to enter the data.
  - More details (e.g. eligible criteria, how to apply, pricing, etc.) will be made available at a later date.

Next Steps

- If you are already using a HIMS
  - Check if your HIMS is HIA-Compliant at https://for.sg/hchlist
  - If your HIMS is HIA-Compliant → Continue using your HIMS.
  - If your HIMS is not HIA-Compliant:
    - Ask your HIMS provider if they are in the process of being certified.
    - Consider switching to a HIA-compliant HIMS.

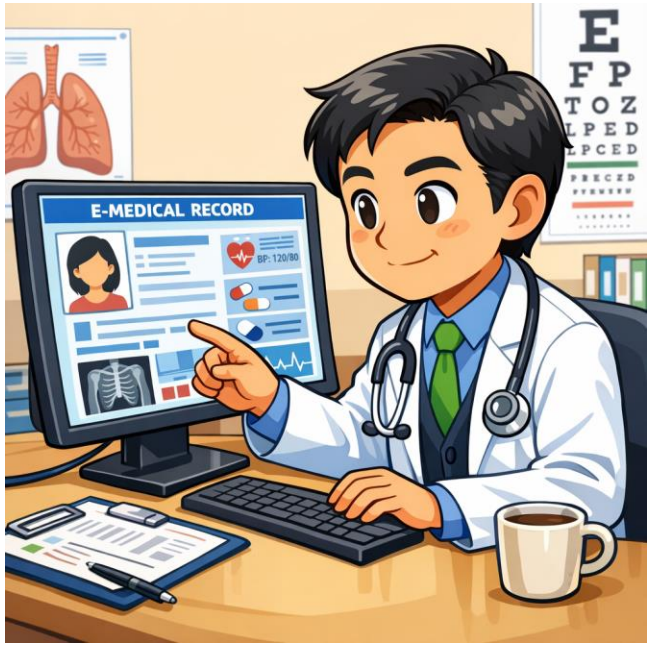
- If you are currently not using a HIMS
  - Keep an eye on the above list and select a HIA-Compliant HIMS when available.
  - Your HIMS Partner will work with you to start contributing to NEHR.
  - We strongly encourage all licensees to adopt a HIA-Compliant HIMS.
  - For eligible clinics who have difficulties and need more time, MOH will offer an alternative contribution solution for submission.

MINISTRY OF HEALTH
SINGAPORE

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

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.

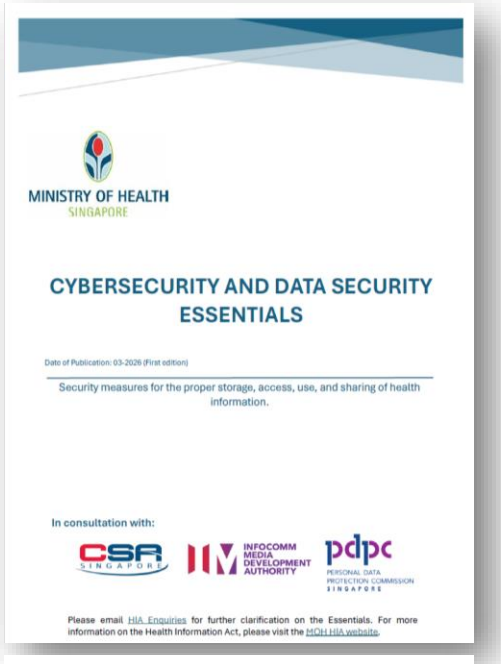
B. **Secure your digital foundation** when you implement cybersecurity and data security measures and defend against system compromises and breaches.

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.

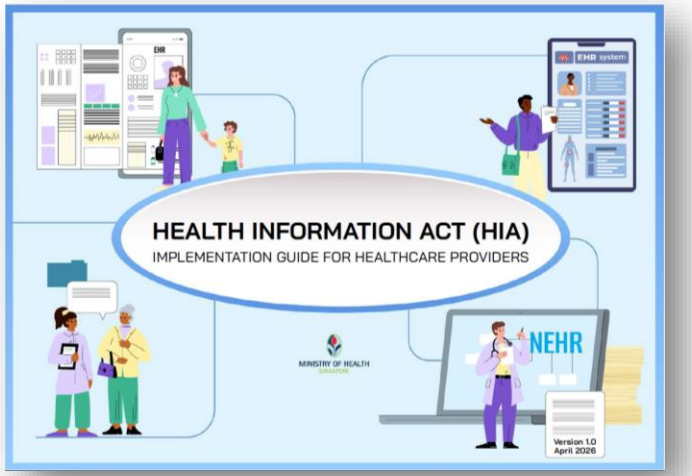
(2) Resources to help you understand and comply with the HIA

Issued in March 2026



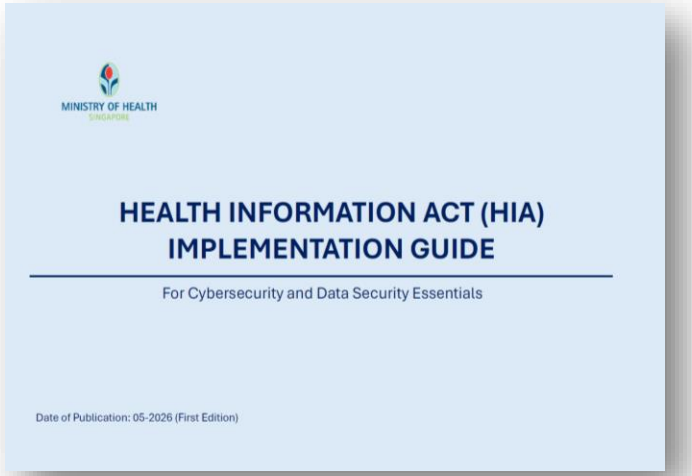
- Mandatory security measures for processing and managing health information.
- Replaced 2023 CS/DS Guidelines.

Issued in April 2026 (Release 1)



- Chapter 1: Overview of what healthcare providers need to do under the HIA, and by when.
- Chapter 2: Steps to take for NEHR contribution and access, with information on the NEHR Connect Grant (NCG).
- Chapter 3a: Overview of cybersecurity and data security requirements (infographic), with information on the types of support available.

Expected mid-2026 (Release 2)



- Release 2 is intended to complement and supplement the CS/CS Essentials.
- Chapter 3b: Implementation guide on cybersecurity and data security measures -
  - Technical steps on cybersecurity measures (e.g. how to turn on anti-virus and firewalls, creating back-ups).
  - Sample cybersecurity and data security corporate clauses.
  - Considerations in setting up a business continuity plan, incident response plan.

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

- **Cybersecurity** focuses on protecting **all the digital information, computer systems, IT and software** your organisation 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.

(5) 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 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.

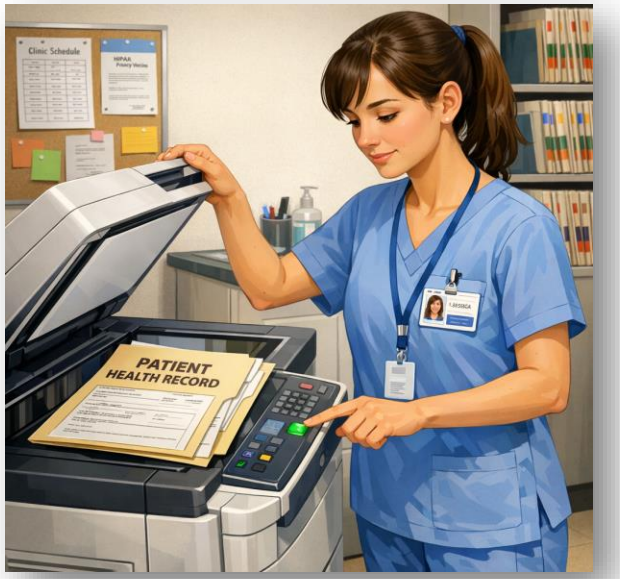
☑ Use only organisation-issued or approved devices to access patient records.
☑ Only install approved applications in the organisation's computers.
☑ Avoid using "end-of-support" hardware or software assets.

(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 clinic.
- ☑ Limit access to hard copy records (on a need-to-know basis) and store them in locked cabinets in your organisation's premises 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.

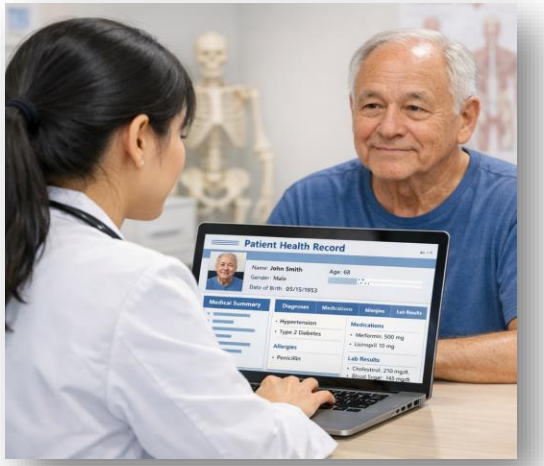
- ☑ Only make copies on a need-to-know basis by authorised parties and for official work purposes.
- ☑ Maintain possession of all copies made (e.g. collect print-outs quickly).
- ☑ Keep health records in your possession at all times when outside the organisation's premises .

(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.

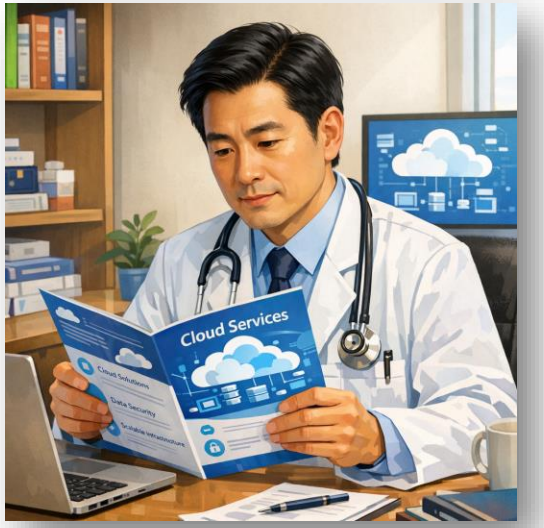
- ☑ The patient must be under your direct care.
- ☑ You have a legitimate need to know to carry out official job functions.
- ☑ You / your staff have been informed or made aware/acknowledge the data protection and security measures under law, corporate policies, and/or professional ethics/standards.

(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 clinic 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 clinic 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 / clinic manager / DPO
Call your IT helpdesk or notify your clinic 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.

(7) Refresher with real-life scenarios - What should you do?

CYBERSECURITY SCENARIO 1

❓ You receive an email that looks like it is from your clinic's IT team asking you to click a link and enter your password.

✓ **Do NOT click the link if it looks suspicious. Report the email to IT immediately. Legitimate IT teams never ask for passwords by email.**

CYBERSECURITY SCENARIO 2

❓ A staff member plugs an unknown USB flash drive found in the office into a clinic computer to check its contents.

✓ **Never use unknown USB drives. Only connect authorised devices to access patient data.**

DATA SECURITY SCENARIO 1

❓ You print a patient's referral letter and leave it on the shared printer while you take a phone call.

✓ **Retrieve letter from printer immediately. NEVER leave patient records unattended - even for a moment.**

DATA SECURITY SCENARIO 2

❓ You look up an old patient's health record out of curiosity.

✓ **Access is RESTRICTED to patients under your current care with a clinical and work reason, and with a need to know.**

MINISTRY OF HEALTH
SINGAPORE

Support Available for the Journey

An initiative of FORWARD SG

Support Available For Healthcare Providers

Support for NEHR Contribution

- NEHR Connect Grant (NCG)
- Alternate Contribution Channel (ACC)
- Guidelines on Appropriate Contribution, Use and Access to NEHR

Support for Cybersecurity and Data Security (CS/DS) Implementation

- Implementation resources and Training Course
- Funding support for CS/DS Implementation
- Funding support to procure cybersecurity solutions

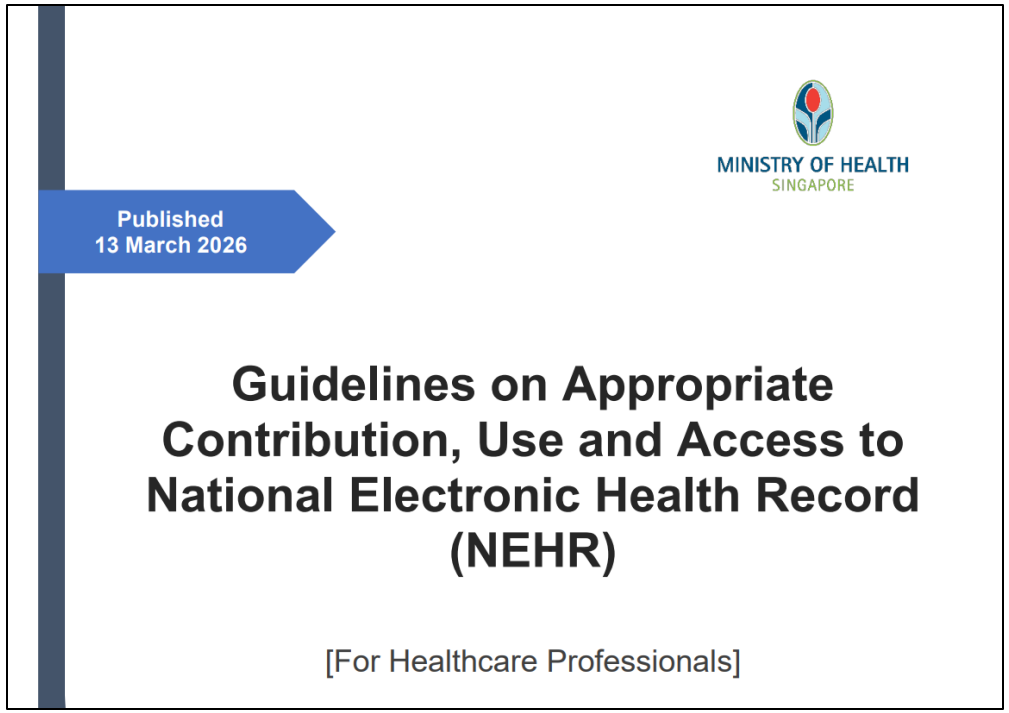
Note: For Community Care Organisations (CCOs), please refer to ANNEX B for available funding support.

NEHR Connect Grant (NCG)

What it is for	To help healthcare providers enhance their existing Health Information Management System (HIMS) or adopt a HIMS that is able to securely contribute to the NEHR
Who is eligible	• Healthcare providers with valid HCSA or HSA license and mandated for NEHR contribution under HIA • Must have selected a HIA-compliant Health Information Management System (HIMS) certified by Synapxe at the point of application • Have not obtained funding from previous MOH grants (e.g. GPITE, NHELP, NH IT) • Not owned by government agency, or MOHH entities
Amount of Support	• **Refer to ANNEX C for NCG grant quantum by service type**
Availability	<table><tr><th>Batch Implementation</th><th>Application Start</th><th>Application Close</th></tr><tr><td>**Batch 1**</td><td>Jul 2026</td><td>Aug 2027</td></tr><tr><td>**Batch 2**</td><td>Aug 2027</td><td>Aug 2028</td></tr><tr><td>**Batch 3**</td><td>May 2029</td><td>Feb 2030</td></tr></table> An online application portal will be launched once the application has opened.

NEHR Guidelines on Appropriate Contribution, Use and Access to NEHR

This set of guidelines aims to assist healthcare professionals in navigating their interactions with NEHR, taking into account the obligations that will apply to healthcare providers and NEHR users under the HIA.



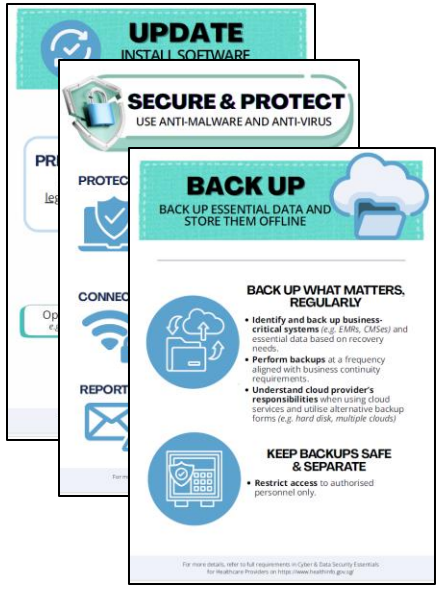
Available on HIA Website: [Guides and Guidelines]

Self-Service CS/DS Implementation Support

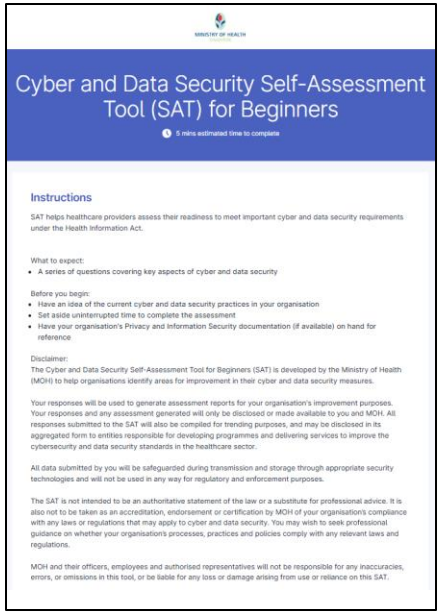
Resources will be progressively made available on HIA Website (www.healthinfo.gov.sg)

https://go.gov.sg/hia-website

CS/DS Infographics

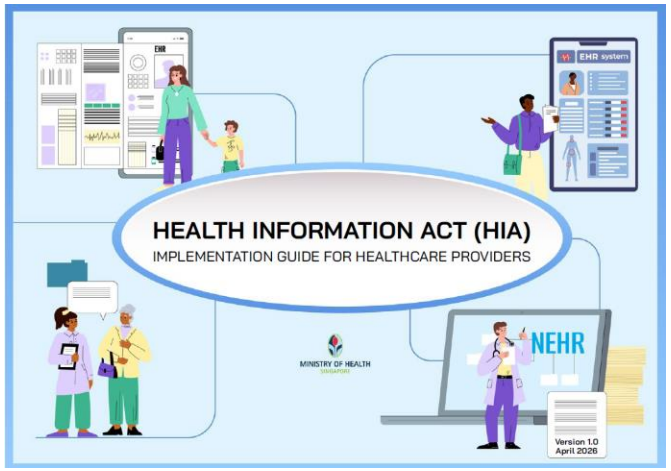


CS/DS Self-Assessment



CS/DS Training Course

HIA Implementation Guide



Assisted CS/DS Implementation Support – CS/DS Service Providers

- Healthcare providers who lack the technical capabilities or prefer to engage professional providers to implement the CS/DS security measures may wish to approach any of the CS/DS service providers onboarded with Cyber Security Agency of Singapore (CSA) in the list linked below:

  CISO-as-a-Service for HIA CS/DS Essentials

- Onboarded CS/DS service providers have demonstrated technical competencies and proven track records in implementing cybersecurity and data security measures.

- MOH does not endorse or recommend any particular organisation, individual, product, process, or service set out above, nor can MOH assure the quality of the work of any organisation or individual. **Organisations should conduct their own due diligence and exercise judgment in selecting the appropriate CS/DS provider.**

CS/DS professional or retainer services are optional as not all healthcare providers will need them. Discuss with service providers on the scope of professional services required depending on your business needs.

Funding Support From Cyber Security Agency of Singapore (CSA): CISO-as-a-Service for HIA Cybersecurity & Data Security Essentials

What it is for	For those who need additional help to meet cybersecurity and data security (CS/DS) requirements by subsidising the cost of hiring qualified CS/DS consultants.
Who is eligible	Small and Medium Enterprises (SMEs)
Amount of Support	• Eligible organisations that apply for CISOaaS will get up to 50% funding support • Eligible organisations that apply for CISOaaS with CE certification will get up to 70% funding support + support for certification fees
Availability	Now
How to apply	Apply via IMDA's CTOaaS portal: https://services2.imda.gov.sg/ctoaas/tag/hia

SMEs refer to businesses registered in Singapore with **≤S$100m turnover OR ≤200 employees**

Price List Of Basic Packages offered by CS/DS service providers

Providers of CISO as-a-Service for Health Information Act (HIA) Cybersecurity and Data Security Essentials – as of 27.03.2026^

^ By default, providers are listed, in descending order, based on the no of projects supported the previous year, i.e. providers listed on top have supported larger no of projects

Cybersecurity and data security consultancy service (with CSA funding support) that is pre-scoped to align to measures in Health Information Act (HIA) Cybersecurity and Data Security Essentials. A cybersecurity health plan will be developed to help the Health Information Act (HIA) entities and Health Information Management System (HIMS) vendors comply with these requirements.

Rank by no. of customers	Name of Provider *(sorted by track records)*	Contact Name	Email	Contact #	Quantity of Endpoints *Price per additional 100 endpoints* Filter via range of endpoints	One-time Professional Service Fees (S$)				Retainer Fees (S$)			
						HIA		HIMS		HIA		HIMS	
						After funding support	Before funding support	After funding support	Before funding support	Retainer Fees (S$ per man-hour)	Retainer Fees (S$ per month)	Retainer Fees (S$ per man-hour)	Retainer Fees (S$ per month)
1					(a) 1 - 5 endpoints	$1,656.00	S$5,520.00	$1,721.00	S$5,736.00	$90.00	$400.00	$90.00	$520.00
					(b) 6 - 10 endpoints	$1,929.00	S$6,240.00	$2,210.00	S$6,672.00	$90.00	$400.00	$90.00	$520.00
					(c) 11 - 20 endpoints	$2,978.00	S$8,840.00	$3,079.00	S$9,452.00	$90.00	$600.00	$90.00	$780.00
					(d) 21 - 50 endpoints	$6,001.00	S$15,340.00	$6,471.00	S$16,402.00	$90.00	$1,200.00	$90.00	$1,560.00
					(e) 51 - 100 endpoints	$8,761.00	S$23,400.00	$9,652.00	S$25,020.00	$90.00	$2,000.00	$90.00	$2,600.00
					(f) 101 - 200 endpoints	$14,802.00	S$36,400.00	$16,408.00	S$38,920.00	$90.00	$4,000.00	$90.00	$5,200.00
					(g) 201 - 500 endpoints*		$18,200.00		$19,460.00	$90.00	$1,200.00	$90.00	$1,560.00
					(h) Above 500 endpoints*		$18,200.00		$19,460.00	$90.00	$1,200.00	$90.00	$1,560.00
2					(a) 1 - 5 endpoints	$1,470.00	S$4,900.00	$1,560.00	S$5,200.00	$100.00	$500.00	$100.00	$500.00
					(b) 6 - 10 endpoints	$1,470.00	S$4,900.00	$1,560.00	S$5,200.00	$100.00	$500.00	$100.00	$500.00
					(c) 11 - 20 endpoints	$1,470.00	S$4,900.00	$1,560.00	S$5,200.00	$100.00	$560.00	$100.00	$560.00
					(d) 21 - 50 endpoints	$2,790.00	S$9,300.00	$2,940.00	S$9,800.00	$210.00	$1,140.00	$210.00	$1,140.00
					(e) 51 - 100 endpoints	$4,764.00	S$15,880.00	$5,064.00	S$16,880.00	$320.00	$1,980.00	$320.00	$1,980.00
					(f) 101 - 200 endpoints	$6,840.00	S$22,800.00	$7,440.00	S$24,800.00	$590.00	$3,180.00	$590.00	$3,180.00
					(g) 201 - 500 endpoints*		$8,000.00		$9,000.00	$320.00	$1,680.00	$320.00	$1,680.00
					(h) Above 500 endpoints*		$12,000.00		$13,000.00	$360.00	$1,680.00	$360.00	$1,680.00

Quantity of endpoints refers to the number of IT hardware that need to be secured (e.g. laptop, desktop)

Basic package price for healthcare providers after 70% funding support

Retainer fees for healthcare providers who need on-going support (optional)

Healthcare providers should **report unethical conduct by service providers** directly to MOH at HIA-related feedback or enquiries

Funding Support From Enterprise Singapore (EnterpriseSG): Productivity Solutions Grant (PSG)

What it is for	To help defray the cost of purchasing solutions to meet CS/DS requirements. (E.g. firewall, antivirus software)
Who is eligible	Small and Medium Enterprises (SMEs) More details: Productivity Solutions Grant (PSG)
Amount of Support	50% of cost of package capped at $30k
Availability	Now
How to apply	Apply via Business Grants Portal: https://www.apply.gov.sg/grants/business

SMEs refer to businesses registered in Singapore with **≤S$100m turnover OR ≤200 employees**

- 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

ANNEX A –
First Schedule: Contribution of Health Information by Specified Contributors

First Schedule: Contribution of Health Information by Specified Contributors
Part 1: Specified Contributors and Types of Health Information to be Contributed

Type of Health Information	Specified Contributor or Class of Specified Contributors												
	Acute Hospital	Ambulatory Surgical Centre	Assisted Reproduction	Clinical Laboratory	Community Hospital	Contingency Care	Nuclear Medicine	Nursing Home	Outpatient Dental	Outpatient Medical	Outpatient Renal Dialysis	Radiological	Retail Pharmacy
Visit Event	✓	✓	✓	—	✓	✓	—	✓	✓	✓	✓	—	—
Adverse Drug Event History	✓	✓	✓	—	✓	✓	✓	✓	✓	✓	✓	✓	✓
Ordered (prescribed) Medications	✓	✓	✓	—	✓	✓	✓	✓	✓	✓	✓	✓	✓
Dispensed Medications	✓	✓	✓	—	✓	✓	✓	✓	✓	✓	✓	✓	✓
Medication List	✓	✓	✓	—	✓	✓	—	✓	✓	✓	✓	—	✓
Vaccines Administered	✓	✓	—	—	✓	✓	—	✓	✓	✓	✓	—	✓
Cardiac Report	✓	✓	✓	—	✓	✓	✓	✓	✓	✓	✓	✓	—
Surgical Procedure Notes	✓	✓	✓	—	✓	✓	✓	✓	✓	✓	✓	✓	—
Dental Notes	✓	✓	—	—	—	—	—	—	✓	—	—	—	—
Visit Diagnoses / Reasons for visit or Patient Problem List	✓	✓	✓	—	✓	✓	—	✓	✓	✓	✓	—	—
Discharge Summary	✓	✓	✓	—	✓	✓	—	✓	—	—	—	—	—
Emergency Department / Urgent Care Summary	✓	—	—	—	—	—	—	—	—	—	—	—	—
Referral Memorandum	✓	✓	✓	—	✓	✓	—	✓	✓	✓	✓	—	—
Laboratory Test Reports	—	—	—	✓	—	—	✓	—	—	—	—	—	—
Radiology / Imaging Reports	—	—	—	—	—	—	✓	—	—	—	—	✓	—

ANNEX B –
Funding Support for Community Care Organisations (CCOs)

Support Available For Non-HCSA Licensed CCOs

Funding Source	Scheme	What It Covers
National Council of Social Service (NCSS)	Transformation Sustainability Scheme (TSS)	Cybersecurity & Data Protection Certifications (DPE / DPTM / CEM/ CTM) • Eligible Social Service Agencies (SSAs) up to $40,000
Cyber Security Agency of Singapore (CSA)	CISO-as-a-Service (for consultancy)	Consultancy for cybersecurity + data security requirements • Eligible SMEs up to 70% co-funding
Enterprise Singapore (ESG)	SMEs Go Digital / Productivity Solutions Grant (PSG)	Pre-scoped IT solutions, equipment & consultancy services to improve productivity (incl. cybersecurity solutions) • Funded up to 50%
Agency for Integrated Care (AIC)	Community Silver Trust (CST)	For eligible Social Service Agencies (SSAs), it is possible to tap on CST for additional cost not covered by NCSS funding, subject to the project meeting the Qualifying Use.

ANNEX C –
NEHR Connect Grant (NCG) Grant Quantum

NCG Grant Quantum By Service Types

Type of Healthcare Service	Grant Quantum per Licensee
Acute Hospital	40% of cost capped at $200k
Clinical Laboratory	40% of cost capped at $140k
Radiological	$12k (fixed amount)
Nuclear Medicine	$8.4k (fixed amount)
Outpatient Medical Services	$8.4k (fixed amount)
Renal Dialysis Centre	40% of cost capped at $29.3k
Contingency Care Services	$8.4k (fixed amount)
Nursing Home	$14.4k (fixed amount)
Assisted Reproduction Services	$8.4k (fixed amount)
Ambulatory Surgical Centre	$8.4k (fixed amount)
Outpatient Dental	$8.4k (fixed amount)
Retail Pharmacy	40% of cost capped at $16.9k