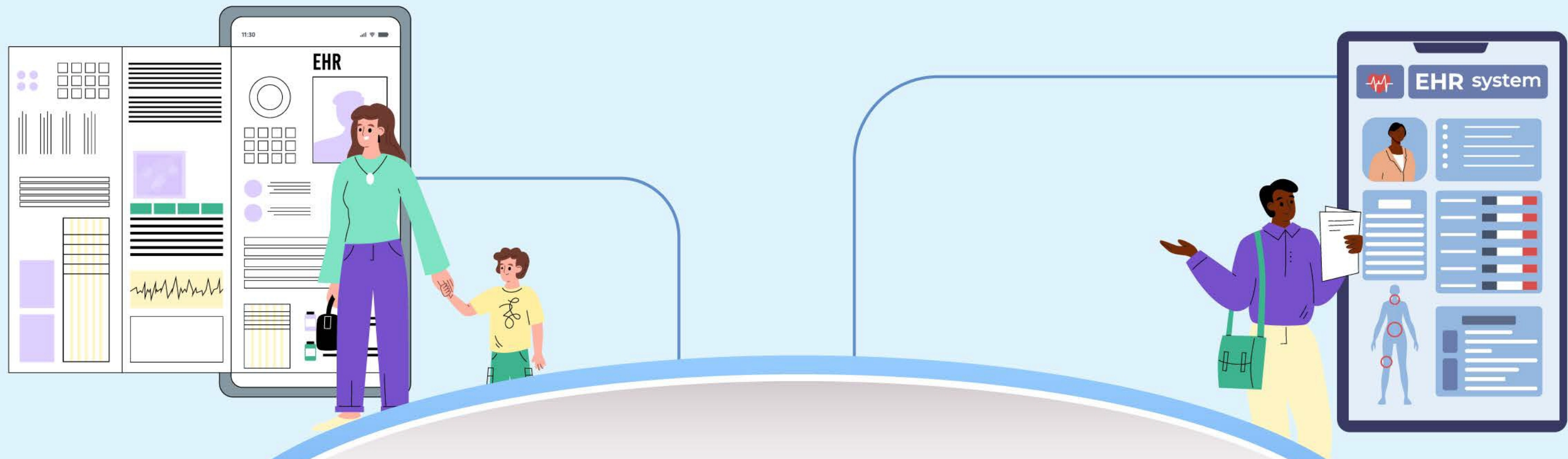




HEALTH INFORMATION ACT (HIA)

IMPLEMENTATION GUIDE FOR HEALTHCARE PROVIDERS



Objective

This Implementation Guide provides healthcare providers with essential information to prepare for the Health Information Act (HIA) requirements.

STRUCTURE OF THE GUIDE

The guide is structured as follows:

- **Chapter 1:** HIA Overview, including on Financial Support
- **Chapter 2A:** Accessing Health Information on the NEHR
- **Chapter 2B:** Contributing Health Information to the NEHR
- **Chapter 2C:** NEHR Connect Grant (NCG)
(Financial Support for HIMS Adoption)
- **Chapter 3:** Cybersecurity and data security measures to protect health information
- **Annex A:** Technical steps to implement cybersecurity measures
- **Annex B:** Sample corporate policy clauses to implement cybersecurity and data security measures
- **Annex C:** Sample data disclosure and confidentiality clauses for agreements with employees and/or third parties
- **Annex D:** Key considerations to formulate a Business Continuity Plan (BCP)
- **Annex E:** Considerations to formulate an Incident Response Plan (IRP)
- **Annex F**
- **Resources**

One Patient, One Health Summary, One Care Journey

The Health Information Act helps healthcare providers access key health information of their patients, making it easier to coordinate care across hospitals, clinics, and community healthcare services. This means fewer duplicate tests, lower costs and safer, higher quality care through complete medical histories that prevent medication errors.

THREE KEY FRAMEWORKS UNDER THE HIA

1 NEHR Contribution and Access

All licensed healthcare providers and retail pharmacies must contribute key health information about patients to the National Electronic Health Record (NEHR) system. They will also be granted access to support care continuity and patient safety.

2 Sharing of Non-NEHR Health Information

The HIA will enable the sharing of non-NEHR health information within the healthcare ecosystem to facilitate community-based care. This is currently only applicable to public healthcare institutions, cluster HQs, AIC and public agencies.

3 Protection of Health Information

Healthcare providers and Health Information Management Systems (HIMS) must put in place reasonable safeguards to ensure confidentiality, integrity, and availability of health information and meet incident notification obligations. The detailed cybersecurity and data security measures are set out in the [Cybersecurity and Data Security Essentials](#).

When You Need to Be Ready

Your implementation timeline depends on your service type:

Table 1: Batched Implementation Timeline		
Service type		
BATCH 1	BATCH 2	BATCH 3
● Outpatient Medical Service (GP) ● Acute and Community Hospital ● Clinical Laboratory ● Radiology Laboratory ● Nuclear Medicine Service	● Outpatient Medical Service (Specialist) ● Nursing Home ● Contingency Care Service ● Outpatient Renal Dialysis	● Outpatient Dental ● 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: For healthcare providers providing multiple service types, NEHR contribution and CS/DS requirements apply according to each service's respective implementation timeline.

For Other HCSA Licensees and Approved Users of NEHR

HCSA licensees not listed in Table 1, which include cord blood banking, human tissue banking, emergency ambulance, and medical transport services, are not required to contribute to NEHR, but need to implement the cybersecurity and data security measures by September 2028.

Financial Support Available

To help you identify the appropriate funding support for NEHR data contribution and meeting cybersecurity and data security requirements, an overview of the available funding schemes is in Table 2. Detailed information about the NEHR Connect Grant (NCG) can be found in [Chapter 2C, page 9](#).

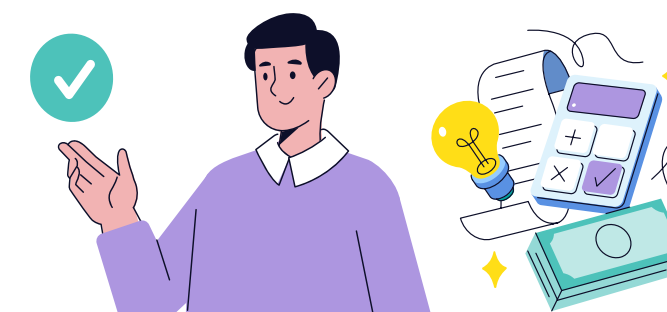


Table 2: Available Funding Support Schemes

	NEHR Connect Grant (NCG)	CISO-as-a-Service ¹ for HIA (Cybersecurity and Data Security Essentials)	Productivity Solutions Grant (PSG)
Ministry/Agency	Ministry of Health (MOH)	Cyber Security Agency of Singapore (CSA)	Enterprise Singapore (EnterpriseSG)
What it is for	To help healthcare providers enhance their existing Health Information Management System² (HIMS) or adopt a HIMS that is able to securely contribute to the NEHR. *For more info: Read here.	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. *For more info: CISOaaS for HIA CS/DS	To help defray the cost of purchasing solutions to meet CS/DS requirements. (E.g. firewall, antivirus software) *For more info: Productivity Solutions Grant (PSG)
Who is eligible	- Licensees with valid Healthcare Services Act (HCSA) / Health Sciences Authority (HSA) Retail Pharmacy licences mandated for NEHR contribution under HIA. - Must have selected HIA-compliant HIMS certified by Synapse. - Exclude those with previous MOH grants (e.g. GP IT Enablement Grant, NHELP, NH IT) and government/MOHH entities.	Small and Medium Enterprises (SMEs)	Small and Medium Enterprises (SMEs)

¹ Chief Information Security Officers as-a-Service (CISOaaS)

² Health Information Management System (HIMS) is the digital system that allows healthcare providers to store and manage patient records

Table 2: Available Funding Support Schemes

	NEHR Connect Grant (NCG)	CISO-as-a-Service for HIA (Cybersecurity and Data Security Essentials)	Productivity Solutions Grant (PSG)
Amount Provided	Approximately 2 years of subscription to a HIMS or up to 40% of the cost of enhancing an existing HIMS.	Up to 70% of the cost of CS/DS Consultancy packages	50% of cost of package capped at \$30k
Availability	Progressively from July 2026 (starting from OMS GP clinics)	Now	Now
How to apply	Apply via OurSG Grants Portal: https://oursggrants.gov.sg	Apply via IMDA's CTOaaS portal: https://services2.imda.gov.sg/ctoas/tag/hia	Apply via Business Grants Portal: https://www.apply.gov.sg/grants/business

National Council of Social Service (NCSS) Members

If your organisation is a member of the National Council of Social Service (NCSS), you can access the Transformation Sustainability Scheme (TSS) – Part C:

Organisation Type	NCSS Members
Scheme Name	Transformation Sustainability Scheme (TSS) – Part C
Funding Coverage	80% funding for CISOaaS consultancy and certification fees
Grant Cap	\$40,000
Requirements	Must attain Cyber Essentials (CE) Mark

How to Apply

Contact NCSS directly or visit their website <https://www.ncss.gov.sg/grants/organisation-development/transformation-sustainability-scheme/>

Staying Updated and Getting Help

Always check the HIA website (<https://www.healthinfo.gov.sg/>) and official MOH circulars for the latest updates. Make sure your primary contact details registered under your HCSA licence are current.

2A) ACCESSING HEALTH INFORMATION ON THE NEHR

The NEHR contains health information which serves as a supplementary tool for healthcare providers. Healthcare providers who wish to apply for access to the NEHR should do it through the System Operator – Synapse.

Follow these steps to get NEHR Access:

1 Check your eligibility (Who can apply for access)

- Determine your organisation's NEHR access eligibility based on your healthcare service type as listed in the [Second Schedule of HIA](#).
- Identify which staff roles in your organisation are authorised to access patient records - typically clinical staff directly involved in patient care such as doctors, nurses, and pharmacists.
- For Intermediate and Long-Term Care (ILTC) services that are interested to access data to the NEHR, please get in touch with the Agency for Integrated Care (AIC) to check your eligibility.

2 Check your participation status

- Verify your institution's NEHR participation status by searching the official participating institutions directory [here](#).
- If your institution is not yet participating:
 - Submit your participation request using the [online application form](#) then register for the mandatory 30-minute virtual onboarding session at [this link](#).

3 Account application

- You will need to apply for an account for each of your users. Apply [here](#).

(Note: Each individual user will need their own account which should be used only when providing care for the specific institution. Users who provide care at different institutions will require a separate account for each institution.)

For assistance:

Contact the NEHR team at NEHR.Feedback@synapse.sg.

Guiding Principles for Access and Use of NEHR Information

REMEMBER: NEHR IS A SUPPORT TOOL, NOT A REPLACEMENT

NEHR does not replace good clinical practice and professional judgement, which includes history-taking and physical examination. There is no need for healthcare professionals to access NEHR for every single consultation. NEHR is an adjunctive source of information for healthcare professionals if they require further information about the patients or if patients cannot recall their information clearly.

Refer to the [Guidelines on Appropriate Contribution, Use and Access to NEHR](#) (published online 13 March 2026) which provides core ethical principles and reasonable professional standards to adopt when contributing to, accessing the NEHR.

Refer to [Annex F](#) which provides policy on the use of the NEHR for institutions to adapt.

2B) CONTRIBUTING HEALTH INFORMATION TO THE NEHR

1) HIA OVERVIEW

2A) ACCESSING NEHR

2B) CONTRIBUTING TO NEHR

2C) NEHR CONNECT GRANT (NCG)

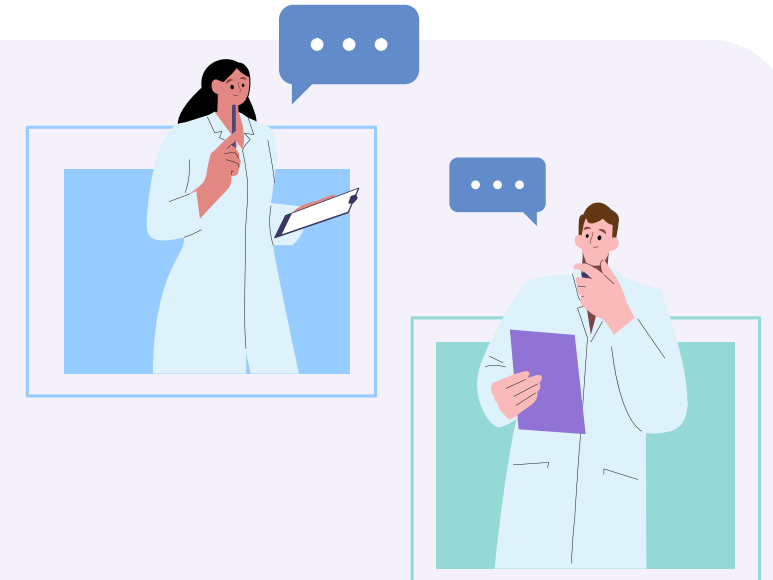
3) PROTECTING HEALTH INFORMATION

ANNEX
A B C D E F

RESOURCES

WHAT YOU NEED TO DO AS A HEALTHCARE PROVIDER: YOUR 3-STEP CHECKLIST

Selected healthcare providers are required to contribute certain data types to the NEHR, based on the types of services they are licensed to provide. Healthcare providers should utilise HIA-compliant Health Information Management Systems (HIMS) to contribute health information to the NEHR.



1

CHECK YOUR NEHR CONTRIBUTION REQUIREMENTS

Selected HCSA licensees and Retail Pharmacies are required to contribute selected data types. Identify your specific data contribution requirements based on your licensed healthcare service type [here](#).

2A

HEALTHCARE PROVIDERS USING A HIMS Verify HIMS Compliance Status

Verify your HIMS meets all three certification requirements:

1. Completion of NEHR Connectivity certification
2. Obtain and submit Cyber Essentials (CE) for HIMS or equivalent Certification to NEHR
3. Declare compliance with Code of Practice for Data Portability

Click [here](#) to check your HIMS's HIA-Compliance status

Proceed to Step 3 if your HIMS meets all 3 requirements.

Otherwise, engage your HIMS Provider to check on their plans and progress to be certified as HIA-compliant.

If you are using a custom developed HIMS, contact Synapxe at nehr.vendorengagement@synapxe.sg to enhance your HIMS to be HIA-compliant.

Alternatively, you may consider switching to a HIMS that is HIA-compliant. In this case, you should ensure your existing and new HIMS providers discuss and present a comprehensive data migration plan and transition timeline with you.

2B

HEALTHCARE PROVIDERS NOT USING A HIMS Onboard a HIA-Compliant HIMS

Select a HIA-compliant HIMS, the HIMS provider will work with you to onboard and start contributing to the NEHR.

The list of HIA-compliant HIMS can be found in [this list](#).

Proceed to Step 3 thereafter.

3

COMPLETE NEHR ONBOARDING PROCESS AND START CONTRIBUTING

Work with your HIMS provider to complete the NEHR onboarding process, including drug inventory mapping and deployment scheduling and start contributing to the NEHR. This process requires up to five weeks for completion.

2B) CONTRIBUTING HEALTH INFORMATION TO THE NEHR

Data Contribution Requirements

Under the HIA, healthcare providers are expected to meet specific obligations in relation to the contribution of key health information to the NEHR. This is to ensure that information in the NEHR is available to other care providers and can support their care for their patients.



QUALITY STANDARDS FOR DATA CONTRIBUTION

As a NEHR data contributor, you must ensure your health information submissions are:

Timely

Enter the information into your HIMS in a timely manner.

Compliant with Standards

Use proper clinical coding standards (Systematised Nomenclature of Medicine - Clinical Terms (SNOMED CT), Logical Observation Identifiers Names and Codes (LOINC), Singapore Drug Dictionary (SDD) Work with your HIMS provider to ensure these are properly configured.

Complete

Submit all required data free of errors, with a reason for every visit.

Attributable

The healthcare provider contributing the health information must be identifiable. Work with your HIMS provider to ensure this is properly configured.

Accurate

Check that the patient details are correct before submission.

Correct

Where errors are detected for data that you have contributed, to update them in the HIMS as soon as possible and work with your HIMS provider to re-submit them to the NEHR.

Find comprehensive data quality standards and contribution requirements [here](#).



NEHR Connect Grant (NCG) Details

The NCG helps eligible healthcare providers adopt or enhance Health Information Management Systems (HIMS) to contribute to NEHR.

NCG Application Timeline

Table 4: NCG Application and Implementation Schedule

Healthcare Service	Grant Application Opens	Grant Application Deadline	Must Start Contributing By
Outpatient Medical (GP)	01 July 2026	31 August 2027	01 September 2027
Acute Hospital Clinical Lab Radiology Lab Nuclear Medicine	01 November 2026	31 August 2027	01 September 2027
Outpatient Medical (Specialist) Nursing Home Renal Dialysis Contingency Care	01 August 2027	31 August 2028	01 September 2028
Outpatient Dental Ambulatory Surgical Centre Assisted Reproduction Retail Pharmacy	01 May 2029	28 February 2030	01 March 2030

Note: Dates are subject to change. Check the [HIA website](#) for the most current timeline.

Important Application Requirements

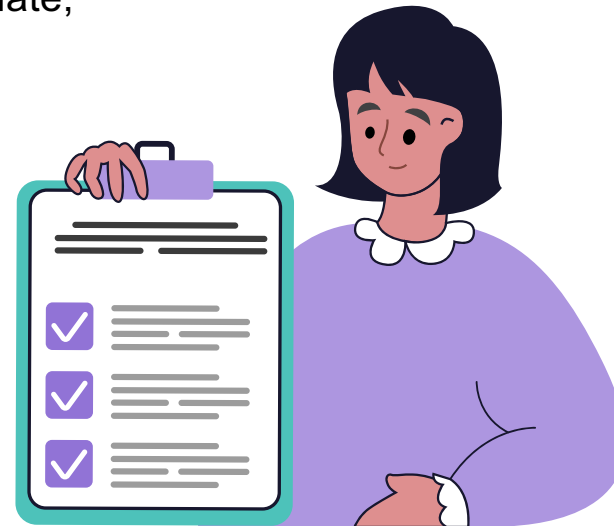
- **Apply Early:** Applications submitted after your enforcement deadline will be rejected
- **HIMS Selection First:** You must select your HIA-compliant HIMS before applying
- **Data Quality Requirements:** You must meet data quality standards for one month to receive full payout
- **Documentation:** All invoices must clearly state which licensable healthcare service the costs relate to

How to Apply

- **Check Eligibility:** Ensure you meet all criteria listed above
- **Select HIA-Compliant HIMS:** Compare HIA-compliant HIMS options by reviewing provider features, costs, and support services. Keep a lookout for the list of certified HIMS provider directory at <https://for.sg/hchlist>
- **Submit Application:** Complete and submit your application online through the OurSG Grants Portal at <https://oursggrants.gov.sg>. *[Note: NCG will be available on the portal once the application has opened.]*

What Happens After Approval

- **Letter of Award (LOA):**
Issued upon application approval
- **Complete Implementation:**
Work with your HIMS provider to start contributing to NEHR
- **Data Quality Monitoring Window:**
Up to 2 months the mandatory contribute date, to meet data quality requirements
- **Submission of Finance Documents:**
Provide required documentation to receive payout
- **Final Payout:**
Processed within 2 months of meeting all requirements and submission of all required documents.



Need Help with Your Application?

- Grants Application Related Enquiries: nehr.grants@synapxe.sg
- Technical HIMS Questions: Contact your selected HIMS provider
- Grant Status Updates: Check the HIA website <https://www.healthinfo.gov.sg/funding-support> for the latest information

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



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.

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

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

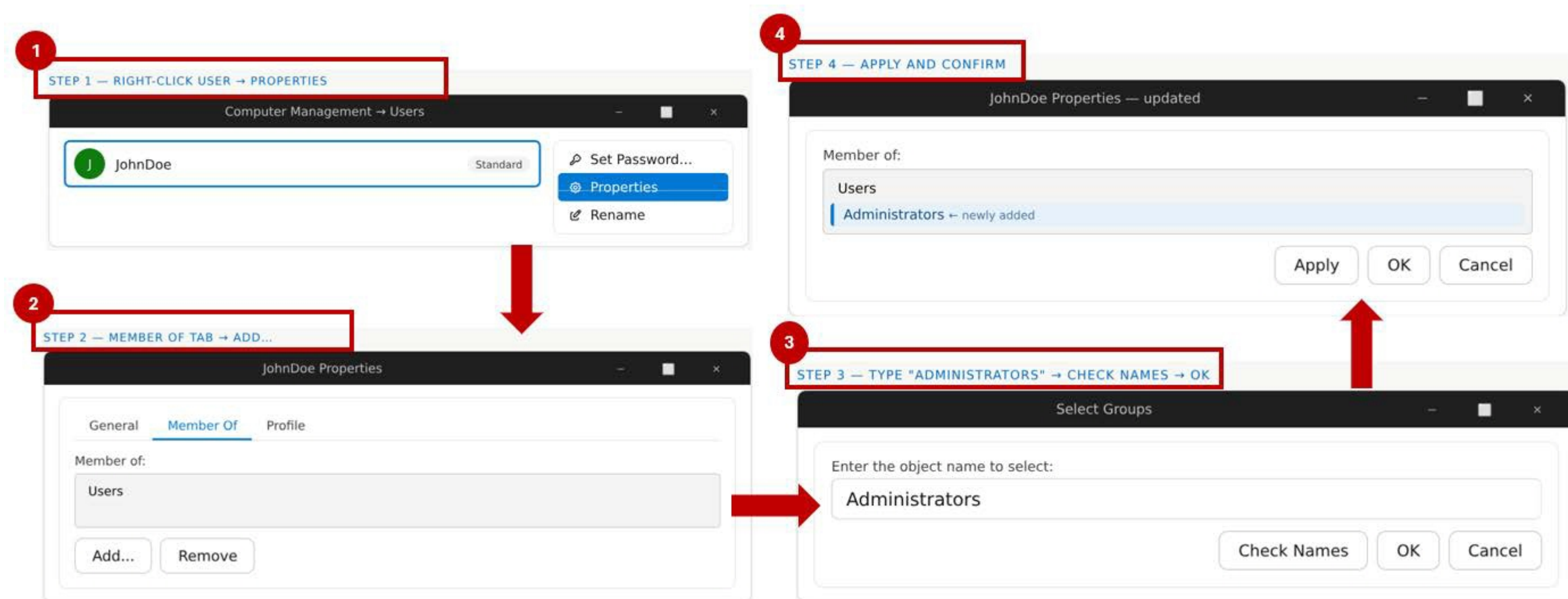
Step 2: What are the resources to help you?

GENERAL	Technical steps (see Annex A
---------	---------------------------------

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

2) STEPS ON GRANTING USER WITH ADMINISTRATIVE RIGHTS

Please follow the steps below to **grant a user administrative rights** after receiving appropriate approval.



3) You conclude the process by having the **third-party user sign a non-disclosure agreement (NDA)**. Please note the document below shows sample key clauses which may be used in your NDA or deed. You must review the sample clauses to assess whether it meets your business and operational needs and contextualise/amend the clauses for your NDA or deed (e.g. to incorporate additional clauses) based on any other business and operational considerations you may have.

<

