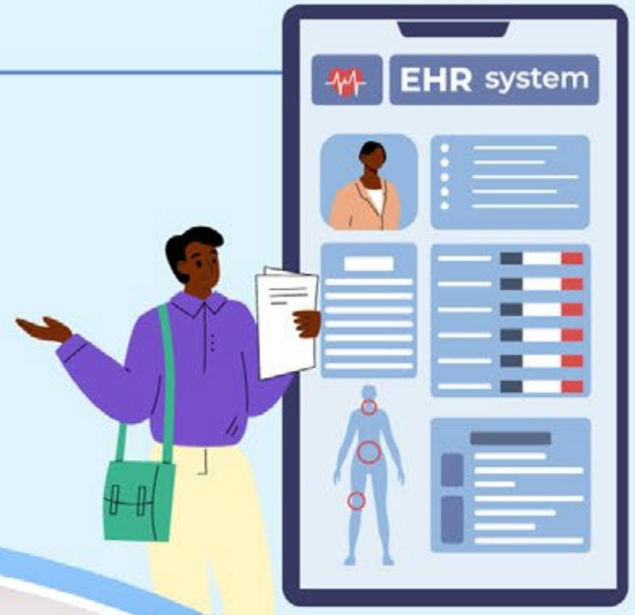


HEALTH INFORMATION ACT (HIA)

IMPLEMENTATION GUIDE FOR HEALTHCARE PROVIDERS

MINISTRY OF HEALTH
SINGAPORE

Version 1.0
April 2026

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 (What You Need to Know and When)
- **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 3A**
  Protecting Health Information
  (Essential Cybersecurity and Data Security Measures)
- ***Chapter 3B & onwards**
  Detailed CS/DS Implementation Steps (Coming Soon)

*This guide will be released in parts: Chapter 3B and onwards will cover practical implementation guidance, corporate policy templates, sample clauses to help healthcare providers implement cybersecurity and data security measures and is scheduled for a May 2026 release.

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) • Private Hospital • Clinical Laboratory • Radiology Laboratory • Nuclear Medicine	• 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 16.

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)
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 System (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	Healthcare providers with valid Healthcare Services Act (HCSA)/Health Sciences Authority (HSA) licences mandated for NEHR contribution under HIA. Must have selected HIA-compliant HIMS certified by Synapxe. 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)

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	**Details will be made available around June 2026**	**Apply via IMDA's CTOaaS portal:** https://services2.imda.gov.sg/ctoaas/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 be do it through the System Operator – Synapxe.

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. Administrative staff generally should not have access rights.
- 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@synapxe.sg.

Guiding Principles for Access and Use of NEHR Information

REMEMBER: NEHR IS A SUPPORT TOOL, NOT A REPLACEMENT

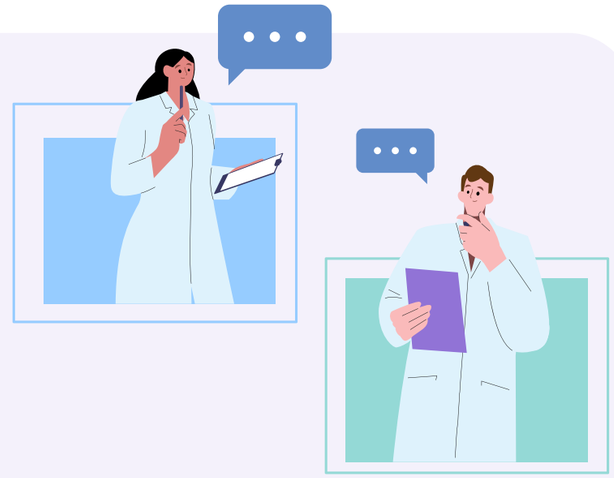
NEHR does not replace good clinical practice and professional judgement, which includes history-taking and physical examination. There is no need for healthcare professionals to access NEHR for every single consultation. NEHR is an adjunctive source of information for healthcare professionals if they 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 which provides policy on the use of the NEHR for institutions to adapt.

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.

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.

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.

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.

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.

Accurate

Check that the patient details are correct before submission.

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.

The NCG succeeds previous digitalisation grants such as the GP IT Enablement Grant and Early Contribution Incentive Grant, both of which have since been closed and were limited to selected licensable healthcare services.

The NCG provides different funding amounts depending on the type of healthcare service. For example, GP clinics operating under the Outpatient Medical Services licence will receive a fixed $8,400 grant.

Table 3: NCG Grant Amounts by Healthcare Service Type

Type of Healthcare Service	Grant Quantum per Licensee
Private Hospital	Up to 40% of cost capped at $200,000
Clinical Laboratory	Up to 40% of cost capped at $140,000
Renal Dialysis Centre	Up to 40% of cost capped at $29,300
Retail Pharmacy	Up to 40% of cost capped at $16,900
Nursing Home	$14,400 (fixed amount)
Radiological	$12,000 (fixed amount)
Outpatient Medical (GP, Specialist) Outpatient Dental Contingency Care Assisted Reproduction Ambulatory Surgical Centre Nuclear Medicine	$8,400 (fixed amount)

What the NCG Covers

- **Purpose:** Support digitalisation and NEHR contribution through HIA-compliant HIMS
- **Coverage:** Approximately 2 years of HIMS subscription or 40% of costs to enhance existing HIMS

Who is Eligible

Healthcare providers must meet **all** of the following criteria:

- Hold a valid HCSA or HSA licence mandated for NEHR contribution under HIA
- Select a HIA-compliant HIMS certified by Synapxe at the point of application
- Have not received previous MOH IT grants (GP IT Enablement Grant, NEHR Early Launch Programme, Nursing Home IT Grant)
- Not owned by government agencies or MOH Holdings entities
- Each healthcare institution can only apply once per licensable healthcare service

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)	July 2026	August 2027	September 2027
Acute Hospital Clinical Lab Radiology Lab Nuclear Medicine	November 2026	August 2027	September 2027
Outpatient Medical (Specialist) Nursing Home Renal Dialysis Contingency Care	August 2027	August 2028	September 2028
Outpatient Dental Ambulatory Surgical Centre Assisted Reproduction Retail Pharmacy	May 2029	February 2030	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/nehrintegratedsystems
- **Submit Application:** Online portal will be available one month before your grant opening date

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 after enforcement 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

In March 2026, MOH published the Cybersecurity & Data Security Essentials to provide guidance on the security measures to be put in place for the proper storage, access, use and sharing of health information. The Essentials are available linked here.

CYBERSECURITY ESSENTIALS

UPDATE PROMPTLY

- Install updates for OS and applications
- Update clinic systems (CMS/EMR)
- Prioritise security patches

PROTECT DEVICES

- Install Anti Malware
- Enable automatic signature update and scanning
- Report suspicious activity

CONNECT SAFELY

- Use firewalls to block unauthorised traffic
- Avoid public networks and use trusted networks
- Use applications only from trusted sources

CONTROL ACCESS

- Unique accounts for all users
- Remove inactive/shared accounts
- Use strong passwords (≥12 mixed characters)
- Enable 2FA for admin/ remote access

ENSURE BACKUPS

- Regular backup of critical and essential data
- Align backups with recovery needs
- Store backups separately

MANAGE ACCESS

- Maintain hardware & software inventory
- Replace unsupported assets
- Authorise new IT assets

DATA SECURITY ESSENTIALS

STORE SECURELY

- Store records in secure, access-controlled locations
- Lock devices storing health info
- Apply confidentiality clauses for staff and vendors

CONTROL ACCESS

- Personnel should only access health info of patients under their care
- Personnel should acknowledge their data protection and security obligations before given access to health info
- Use screen-locks and privacy filters

TRANSFER SECURELY

- Password-protect files containing health info before sending by email
- Send the passwords through a different channel
- Check recipients' email addresses before sending.

COPY SECURELY

- Copies of health info should only be made by authorised personnel, and where necessary for work purposes
- Maintain possession of all copies of health info made at all times

COMMON CYBERSECURITY & DATA SECURITY ESSENTIALS

TRAIN PERSONNEL

- Ideally attend annual cybersecurity and data security training
- Develop basic cybersecurity and data security hygiene practices for personnel to adopt

MANAGE THIRD PARTIES

- Understand the security services that IT service providers will provide, and ask for regular updates on security issues
- Understand the remaining steps that you need to take (e.g. configurations)
- Check service providers' certifications and safeguards

REVIEW SECURITY

- Review CS/DS measures periodically
- Review compliance with security measures
- Act promptly upon lapses

SECURE DISPOSAL

- Shred physical records when no longer required
- Encrypt or overwrite electronic records

BUSINESS CONTINUITY

- Prepare for disruptions (e.g. when IT systems are compromised)
- Establish a continuity plan to ensure resilience

INCIDENT RESPONSE

- Set out clear roles and responsibilities for key personnel
- Detect, respond and recover from incidents
- Communicate with affected persons and regulators

Looking Ahead: Additional Resources Coming Soon

Your HIA implementation journey doesn't end here. We are continuously developing additional resources to support you every step of the way.

What's Next: Chapter 3B and onwards

In the next release of this Implementation Guide, Chapter 3B: Detailed CS/DS Implementation Steps, further information will be provided:

- Guides on how to implement cybersecurity measures e.g. enable security features on your computers
- Suggested corporate policy templates to implement policies and practices for cybersecurity and data security measures
- Other resources to help operationalise cybersecurity and data security measures at a practical level

<NAME OF INSTITUTION> POLICY ON THE USE OF THE NATIONAL ELECTRONIC HEALTH RECORD (NEHR)

1. Aim

1.1. This policy serves to guide authorised individuals of the NEHR on the proper use of the NEHR and the handling of their NEHR accounts.

2. Applicability

2.1 This policy applies to all individuals who have been provided access to the NEHR through the organisation.

3. Terms

3.1. Authorised Individuals – Persons who have been approved by this organisation and granted an account to access the NEHR by Synapxe.

4. Access to the NEHR and handling of NEHR Accounts

4.1. Only individuals who have been authorised by the institution and Synapxe are allowed to access the NEHR.

4.2. Individuals should not access NEHR using other individuals' credentials.

4.3. Individuals should not share their NEHR credentials or allow their NEHR credentials to be used by other individuals to access the NEHR.

4.4. Individuals are responsible all activities conducted through their NEHR account and are responsible for safeguarding their credentials used to access the NEHR.

5. Proper use of the NEHR

5.1. Authorised individuals must only access the NEHR Health Information of patients who are officially under the care of this organisation. They should not access the NEHR Health Information of patients who do not have an established official relationship with this organisation, even if the patient as given permission to do so.

5.2. Authorised individuals must not use the NEHR Access provided by this organisation when providing care / working at other organisations. The NEHR account provided by this organisation is for use when the authorised individual carrying out duties for this organisation only.

5.3. Authorised individuals must only access the NEHR for the provision of *healthcare/approved long term care services to this organisation, or for other purposes that have been permitted by the Ministry of Health.

** Please strikethrough where not applicable*

5.4. Authorised individuals must not access the NEHR for purposes relating to employment and insurance, except if the access is for purposes of conducting a medical examination allowed for under the Third Schedule of the Health Information Act.

5.5. Authorised individuals must not access the NEHR for administrative, audit, purely educational, or research purposes unless specifically approved by MOH.

5.6. When writing medical reports, authorised individuals must only access NEHR as part of performing a clinical examination. Authorised individuals should not access NEHR for the sole purpose of writing a medical report in the absence of a clinical examination.

5.7. When NEHR is accessed, there should be proper documentation to support the use of the NEHR in the patient's case notes/ medical records.

6. Handling of NEHR Health Information

6.1. Authorised individuals must not disclose NEHR Health Information to persons outside this organisation.

6.2. Authorised individuals may only disclose NEHR Health Information to person within this organisation if they are providing care to the patient and need the information to provide care to the patient.

7. Termination of NEHR Access

7.1. When a user no longer requires access to the NEHR for his duties. The user or his reporting officer must inform the organisation's authorised officer to terminate the NEHR access of the user.

A set of documents and resources are listed in Table 5 designed to guide you through different aspects of compliance. The table below shows all currently available resources:

Table 5: List of Supporting Documents and Resources

Type of Resource(s):	Link(s):
1) MOH - Information & updates on HIA	Health Information Act
2) 6 March 2026 MOH Circular on the • Overview and Implementation of the Health Information Act (HIA)	Circular - Overview and Implementation of the Health Information Act (HIA)
3) Cybersecurity and Data Security Essentials for Healthcare Providers • Sets out cybersecurity and data security requirements for healthcare providers under the HIA	Cybersecurity and Data Security (CS/DS) Essentials
4) Guidelines on Appropriate Contribution, Use and Access to NEHR • Aims to assist healthcare professionals in navigating their interactions with the NEHR	Guidelines on Appropriate Contribution, Use and Access to National Electronic Health Record (NEHR) (March 2026)
5) Synapxe - connect NEHR website • National Electronic Health Record (NEHR) - Frequently Asked Questions • Participate in the NEHR - Steps to access and contribute to NEHR • Contact Details	Home | Connect to NEHR
6) List of all organisations and institutions that participate in the National Electronic Health Record System (NEHR)	Institutions Participating in the National Electronic Health Record System (NEHR) | Ministry of Health
7) Health Information Management System Integration with NEHR • Check status and compare and select HIA-compliant Health Information Management System vendor	Status of System Integration with the NEHR

Stay Connected

Check the HIA website (https://www.healthinfo.gov.sg/) for updates to this Implementation Guide and available resources.

For questions about your HIA implementation journey, contact the HIA support team at hia_enquiries@moh.gov.sg.

REMEMBER:

HIA readiness is an ongoing process. Each step you take strengthens your ability to deliver secure, high-quality healthcare in our increasingly digital world.