Updated as of 13 August 2026

FAQs for Healthcare Providers on the Health Information Act (HIA)

Table of Contents

NEHR Contribution and Access

1. Do I need to contribute patients' health information that was obtained previously, or do the requirements apply on a prospective basis?

There is no requirement for you to upload historical records. HIA's NEHR contribution requirements apply on a prospective basis.

2. Who should submit clinical laboratory test reports to NEHR – the ordering healthcare provider or laboratory generating the test report?

Under the HIA, licensees are responsible for submitting health information that they generate. As laboratory reports are generated by the clinical laboratories, clinics and other ordering providers are not required to submit the laboratory reports.

The clinical laboratories that generate and issue the reports will be required to contribute the reports to the NEHR.

3. Do we need to contribute foreign patients' health information to NEHR?

Under the HIA, only the health information of Singaporeans, Permanent Residents and individuals with Foreign Identification Numbers (FIN) need to be contributed to NEHR as these groups are more likely to seek care in Singapore over time. You are not required to contribute health information (e.g. laboratory test results) of short-term foreign visitors to NEHR.

4. Are aesthetic clinics required to contribute health information to NEHR?

Aesthetic clinics hold an Outpatient Medical Service (OMS) licence under the Healthcare Services Act (HCSA) and are therefore required to contribute the relevant health information, specified in the First Schedule of HIA, to NEHR.

5. What is the process for correcting errors in NEHR documentation made by other healthcare providers? Who is responsible for making these amendments?

The original contributing provider bears responsibility for correcting any errors in their documentation. When errors are discovered by healthcare providers, they should notify the original provider who made the entry to facilitate the necessary corrections.

6. Which healthcare professionals are allowed to access the NEHR?

Authorised healthcare professionals working within licensed healthcare institutions, such as doctors, nurses, pharmacists, and allied health professionals, are eligible to access NEHR for the purpose of providing direct patient care.

7. How do I apply for access to the NEHR?

If you are using an electronic medical record (EMR) that is integrated with the NEHR, reach out to your EMR administrator for account provisioning. If your institution is not participating in NEHR yet, you can submit your participation request using this form and complete the virtual onboarding session. You will need to apply for an account for each of your users through this form and send a completed copy to nehr.svcorps@synapxe.sg.

For assistance, you can reach out to nehr.feedback@synapxe.sg.

8. Is it necessary for me to access NEHR for every consultation, and do I need to review the entire NEHR record?

NEHR is meant to serve as an adjunct to a clinical examination. It is an additional source of information in cases where the patient is unsure or is unable to recall information that the provider requires to manage the patient. Providers should use their clinical judgement as to whether there is a need to access the NEHR when examining a patient.

MOH has published the "Guidelines on Appropriate Contribution, Use and Access to NEHR" to support you, by suggesting reasonable professional standards that should be adopted with respect to NEHR. The guidelines will complement existing professional ethical codes (i.e. Singapore Medical Council (SMC) and Singapore Dental Council (SDC) Ethical Code and Ethical Guidelines (ECEG)) and will be updated periodically to reflect developments in the healthcare landscape and clinical practice.

9. Can NEHR be accessed to share information with patients upon their request e.g. by printing out certain records for the patient's retention?

Only healthcare professionals involved in patient care may access NEHR, and NEHR information may only be disclosed to other healthcare professionals involved in caring for the same patient.

You should direct patients requesting NEHR information to view their health records through HealthHub. Alternatively, as NEHR does not contain patients' complete health records, patients may wish to contact the relevant healthcare provider that had provided the care for the information they seek.

10. What is considered appropriate access or use of NEHR?

NEHR can be accessed/used under the following scenarios:

1) For healthcare service delivery EXCEPT for insurance/employment related purposes; OR
2) Specified medical examinations as listed in the Third Schedule of the HIA.

Specifically, on responding to requests by insurers, healthcare professionals should rely on their institution's medical records system, such as those in their Health Information Management Systems (HIMS), or information obtained from patient interactions or examinations, after ensuring that the patient has provided consent for the sharing.

11. What happens if patients have placed Access Restrictions on their NEHR information?

Patients may restrict access to all or select healthcare providers to their information in NEHR. In such cases, only basic information (allergies and vaccination records) will still be accessible to support continuity of care.

Only doctors may 'break-glass' to access NEHR when such Access Restrictions are in place, during medical emergencies. All accesses made to an access-restricted record for medical emergencies will be subjected to audits. Accesses of access-restricted records in non-medical emergencies is a serious offence under HIA.

These enhanced access controls and 'break-glass' feature will be made available from 2027.

12. What protections or clarifications does HIA provide regarding potential medico-legal liabilities that may arise from my use of NEHR information?

Healthcare professionals who access NEHR in good faith, with reasonable care and in accordance with HIA will be granted legal protection in relation to their access and use of NEHR information.

To support you in complying with HIA's requirements, MOH has published a set of guidelines on the appropriate contribution, access and use of NEHR information to address key medico-legal concerns.

Cybersecurity and Data Security

13. How quickly must I notify affected individuals after discovering a data breach?

In general, if a data breach causes or is likely to cause significant harm[1] to an individual or of a significant scale (i.e. 500 or more affected individuals), you should notify the affected individuals upon notifying MOH.

For more information, refer to the link here.

14. What kind of firewalls or antivirus solutions would be enough to meet CS/DS Essentials? Will Microsoft Defender suffice or we need enterprise grade solutions?

The adequacy of security solutions depends on the specific system setup and network complexity. For organisations such as solo practitioners or small clinic chains with simple system setups, Microsoft Defender may provide sufficient firewall protection. This principle applies similarly to antivirus requirements, where built-in operating system security features, such as Microsoft Defender, can meet basic protection needs for less complex environments.

However, organisations should evaluate their specific risk profile in the case of multi-tier architecture when determining whether built-in security solutions adequately address their cybersecurity needs or whether additional enterprise-grade solutions are necessary.

15. Specialists frequently receive referrals containing large amounts of data on thumb drives, which are difficult to scan comprehensively for malware due to their large data volumes. How could the CS requirements be met in this scenario?

Healthcare providers are not required to perform a full, deep-scan of the entire USB content of the thumb drive. Instead, they should ensure their built-in anti-malware systems are configured to provide real-time protection by automatically detecting and scanning for malicious files upon access, through insertion of portable storage media (e.g. USB thumb drives).

16. Is Mobile Device Management (MDM) for Bring Your Own Device (BYOD) programmes a requirement under the HIA?

MDM[2] for BYOD programmes is not a mandatory requirement under the Cybersecurity and Data Security (CS/DS) Essentials. However, computer systems used to access health information, such as NEHR, must meet the CS/DS requirements set out under the CS/DS Essentials.

---

[1] For example, data breaches involving certain health information deemed to be more sensitive, such as those relating to sexually transmitted infections. Details of data breaches that would be deemed as being likely to result in significant harm will be set out in subsidiary legislation to be issued.

[2] MDM (Mobile Device Management) is a security solution that allows organisations to remotely manage mobile devices, enforce security policies, and protect organisational data, allowing personnel to securely access work resources on mobile devices.

17. Can the password of a password-protected file be sent via the same email channel? What would be an appropriate channel to do so?

Passwords should not be sent through the same channel as the protected file. Should the email system be compromised, both the file and its password would be exposed simultaneously, potentially compromising the health information. Passwords should instead be transmitted via a separate channel such as via phone, SMS or an instant messaging application.

18. Patients often communicate with WhatsApp for appointments and results and reports. What is MOH's view on this?

Instant messaging platforms can be used for basic appointment scheduling (e.g. reflecting date and times), without any disclosure of medical information. For communications involving medical information, official company-designated communication channels, such as their office email, are recommended.

19. Is it right to say that adopting a fully HIA-compliant Health Information Management System (HIMS) will help address all my cybersecurity requirements, and I just need to focus on implementing data security / protection measures?

Adopting a HIA-compliant HIMS will help to meet some CS/DS requirements, as well as fulfil requirements relating to NEHR contribution. While adopting a HIA-compliant HIMS helps in securing your software, healthcare providers are still required to align their internal processes and staff workflows to meet HIA's CS/DS requirements. For instance, you need to ensure that staff are familiar with basic cyber practices, such as identifying phishing threats and practicing good password hygiene. MOH will be issuing further guidance and resources (such as practical implementation guidance, corporate policy templates and sample clauses) to support healthcare providers in implementing these cyber and data security requirements.

Support Available

20. What funding and technical support will be provided to help me onboard to NEHR?

MOH will be providing various forms of support to help healthcare providers adopt HIA-compliant Health Information Management Systems (HIMS) and meet HIA's CS/DS requirements.

- **Funding Support**: MOH will provide a one-off grant support for eligible private healthcare providers to onboard to HIA-compliant HIMS to contribute data to NEHR. More details can be found here.
- **Technical Support**: Synapxe will work with your HIMS provider or IT department, which will do most of the heavy lifting on system integration and getting their HIMS certified as HIA-compliant. Your HIMS provider will also support and guide you through the onboarding process.
- **Clinical Support**: You will receive clinical support on content guidance and best practices when implementing clinical standards within your HIMS. This includes Q&A sessions for your HIMS providers and briefing session for clinical users to identify areas where help is required. If you need professional help in drug inventory mapping, sign up for the drug mapping service here.

21. What implementation guidance is available to help me prepare for HIA requirements?

The HIA Implementation Guide supports healthcare providers in preparing for HIA requirements. Release 1 of the HIA Implementation Guide (available here) equips healthcare providers with the essential information needed to prepare for HIA requirements, covering three key areas:

- Contributing to and accessing the NEHR,
- Available financial support schemes, and
- The cybersecurity and data security measures required to protect health information.

Release 2 will cover practical implementation guidance, suggested corporate templates and sample clauses to help healthcare providers implement cybersecurity and data security measures and is scheduled for release by mid-2026.

22. I currently run a practice which is strictly on pen and paper – must I adopt a HIA-compliant Health Information Management System (e.g. Clinic Management System (CMS))?

Healthcare providers are strongly encouraged to digitalise their operations and adopt a HIA-compliant HIMS for more efficient and safer care delivery.

For pen-and-paper clinics which have obtained their licences before 2027 and have difficulties digitalising or require more time to digitalise, MOH will be providing an Alternate Contribution Channel (ACC) to help them comply with the contribution requirement. More details will be provided in due course.

23. Will I be able to implement the CS/DS measures myself? Do I need to engage professional CSDS consultancy services (e.g. CISOaaS)? What is MOH doing to ensure the consultancy services charge appropriately?

Engaging professional CS/DS consultancy services is optional, as not every healthcare provider requires such services to meet the necessary CS/DS requirements. For those who require more help to implement the CS/DS measures, MOH has engaged cyber and data security professional services (i.e. CISOaaS) qualified by Cyber Security Agency (CSA) to develop standardised basic security packages for healthcare providers, with transparent pricing structures. These professional services have been asked to clearly distinguish between services to address essential requirements versus optional services.

Healthcare providers are strongly encouraged to refer to the MOH HIA Implementation Guide for further guidance. Release 2, scheduled for publication in mid-2026, will cover practical implementation guidance, suggested corporate templates, and sample clauses for cybersecurity and data security measures.

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

24. Will MOH be providing template SOPs covering CS/DS Essentials policies and practices? Individual practitioners working towards HIA-readiness may lack the domain expertise to independently develop protocols for unforeseen events like cyber attacks, and such templates would help address this gap.

MOH is currently developing templates that will be incorporated into the HIA Implementation Guide (Release 1 published here). Release 2 of the HIA Implementation Guide, scheduled for publication in mid-2026, will provide practical implementation guidance and suggested corporate policy templates.