Feedback Report on the Public Consultation for the Health Information Bill

5 November 2025

Introduction

1. The Ministry of Health ("MOH") conducted a public consultation on the policies underpinning the proposed Health Information Bill ("HIB") from 11 December 2023 to 11 January 2024.

2. The HIB governs and supports the safe and secure collection, access, use and sharing of health information by healthcare providers across various care settings to support better care continuity and safeguard patient welfare. This will be done by:
    a. Requiring the contribution to and enabling the access to key health information in the National Electronic Health Record system (NEHR);
    b. Enabling the sharing of non-NEHR health information within the healthcare sector to facilitate outreach to and shared care of patients in relation to national programmes such as Healthier SG and Age Well SG; and
    c. Establishing appropriate cybersecurity and data security standards, to safeguard health information.

3. MOH thanks the respondents, including members of the public, healthcare professionals and representatives of healthcare organisations, and Health Information Management System (HIMS) providers[1], who contributed their views. MOH has carefully considered the feedback. This report sets out the key points raised, and MOH's responses including updates to the HIB policies.

Summary of Feedback Received

4. Respondents generally endorsed the HIB, recognising its potential to enable more coordinated care among healthcare teams. Patients will benefit from safer, higher-quality care delivered by healthcare providers who may access a comprehensive overview of patients' medical histories, enabling more accurate diagnoses and better continuity of care across different settings. Patients will enjoy cost savings, reduced waiting times, and a more seamless healthcare experience through the reduction of duplicate tests and procedures when consulting different healthcare providers.

5. Several key themes arose from the feedback, including (A) how health information governed under the HIB would be accessed, used, disclosed, and protected; (B) level of patient control over the contribution of and access to their NEHR records; (C) clarity on the use of NEHR information for purposes beyond patient care; (D) concerns surrounding medico-legal liability of healthcare professionals when accessing NEHR for patient care purposes; and (E) support measures to help healthcare providers meet their legal obligations under the HIB. These themes, together with MOH's responses, are addressed in the following sections.

Key Themes

(A) How health information governed under the HIB would be accessed, used, disclosed and protected

6. Respondents were largely supportive of the proposed cybersecurity and data security requirements and other safeguards, including the need for regular audits on accesses to NEHR. HIMS providers and other organisations felt that the requirements should be robust, though smaller providers (e.g. solo-practitioners) might have some difficulties fulfilling the proposed cyber and data security requirements.

[1] An example of a HIMS provider is a clinic management system vendor.

Table 1: Detailed feedback on the policies regarding the access, use, disclosure and protection of health information and MOH's responses

Feedback	MOH's response
Respondents sought clarity on the level of access granted to healthcare professionals and other persons to patients' NEHR data, as well as the classes of healthcare professionals which may access such data.	Access to NEHR is first and foremost for the delivery of patient care. Access to NEHR will be restricted to select groups involved in the delivery of care ("Healthcare Providers") such as healthcare providers licensed under the Healthcare Services Act 2020 (HCSA); retail pharmacies licensed under the Health Products Act 2007; and selected community health partners who play a critical role in planning for and coordinating the delivery of healthcare services in the community. Healthcare Providers and their authorised personnel are only permitted to access the NEHR information of patients they provide patient care to.
Respondents requested greater clarity and detail on the categories of data required to be contributed to the NEHR.	Only selected health information of Singapore Citizens, Permanent Residents and Long-Term Pass Holders that are essential for ensuring the continuity of care across Healthcare Providers and care settings will be required for contribution to the NEHR. This includes allergies, vaccinations, visit diagnoses and discharge summaries. The list of key health information required to be contributed to NEHR will be published on our website.
Respondents asked for more clarity on how health information governed under HIB will be accessed, used, disclosed, and protected.	There will be controls in place to govern the safe access, collection and use of NEHR information such as: (a) Healthcare Providers and their authorised personnel may only access the NEHR information of patients registered with them; (b) Only personnel directly involved in patient care are granted NEHR access. Thus, Healthcare Providers are required to update MOH when the roles of their authorised personnel change, e.g. when a nurse takes on an administrative, non-patient-care role; (c) There will be penalties to deter unauthorised or improper access and collection of NEHR information; and (d) Accessing NEHR information for employment or insurance purposes (not in compliance with the HIB) will also be disallowed. Patients will be able to limit Healthcare Providers' access to their NEHR information by placing access restrictions.
Respondents noted a need to ensure that the cybersecurity and data security requirements imposed on healthcare organisations are robust.	The HIB will require Healthcare Providers to ensure their cybersecurity and data security practices are robust and fit for purpose. MOH has developed cybersecurity and data security standards designed to help HIB entities maintain basic cyber hygiene, which is essential for defending against common cyber threats. These standards have been reviewed by key regulatory bodies, including Cyber Security Agency (CSA), Infocomm Media Development Authority (IMDA), and Personal Data Protection Commission (PDPC), to ensure their relevance and effectiveness in safeguarding healthcare information and systems.
Some respondents highlighted that breaches of the HIB would need to be dealt with appropriately, to ensure that patient confidentiality is upheld	Enforcement of the HIB will be robust and calibrated taking into account all relevant considerations including the impact of the breach. For instance, the HIB imposes stiff penalties for the unauthorised access and improper use and disclosure of NEHR information.

	Other breaches such as the non-contribution of health information to NEHR could occur due to reasons outside the control of Healthcare Providers such as technical faults in their HIMS. MOH and the NEHR System Operator will first work closely with the Healthcare Provider to address these issues as appropriate. MOH may also first issue a direction for the Healthcare Provider to rectify the non-contribution within a reasonable timeframe, before taking enforcement action if MOH's direction is not complied with. If Healthcare Providers exercised due diligence in selecting a white-listed HIMS, they would not be held accountable for lapses or cybersecurity non-compliances arising solely from these HIMS solutions. Healthcare Providers will still need to ensure their clinic processes and staff are able to meet the cybersecurity and data security requirements under the HIB.

(B) Level of patient control over the contribution of and access to their NEHR records

7. Respondents were largely supportive of the controls put in place for health information. Some queried if greater levels of patient control over the type of health information that is contributed to or accessed via the NEHR would be provided, as this would give greater assurance on patient privacy and confidentiality.

Table 2: Detailed feedback on the policies regarding the levels of patient control over the type of health information contributed to or accessed via the NEHR and MOH's responses

Feedback	**MOH's response**
Respondents queried if additional patient controls would be considered to provide more autonomy in whether certain information would be contributed to or accessed via the NEHR. There were also suggestions for MOH to review giving patients more controls on their own NEHR records, or to institute additional safeguards in relation to access.	Currently, when a patient activates access restrictions on their NEHR information, it is an 'all-or-nothing' design. Once activated, all Healthcare Providers will be blocked from accessing the patient's data, even if there is a medical need or emergency. Following extensive consultations with stakeholders including patient advocacy groups, MOH will revise the access restriction regime to enable greater autonomy and enhance patient safety: (a) We will enable all patients to select the Healthcare Providers who can access their NEHR information. (b) A basic set of key health information (e.g. allergies, vaccination records) will remain accessible to all Healthcare Providers even if an access restriction is in place. This is the critical set of key health information, which should be made available to any healthcare provider to support the clinical care of patients at all times. (c) In the event of a medical emergency that threatens the life or health of the patient, Healthcare Providers may override access restrictions to assess the rest of the health information. This enhances speed and quality of care, which is critical during medical emergencies. It is also a feature in jurisdictions such as Finland, Australia and Hong Kong which have national health repositories similar to NEHR. These enhanced access controls will be made available on the HealthHub application in the second half of 2026. Health information will be contributed to the NEHR even if the patient has placed access restrictions. This ensures that there is no gap in their records

	should they choose to lift access restrictions in future, and that patients receive appropriate care during emergency situations when the healthcare providers need to override the restrictions.

(C) Clarity on the use of the NEHR information for purposes beyond patient care

8. Members of the public, healthcare professionals and representatives of healthcare organisations generally supported the access and use of NEHR data for secondary purposes such as public health research. Concerns were raised in relation to the use of NEHR data for insurance or employment purposes.

Table 3: Detailed feedback on the policies regarding the access and use of NEHR data for circumscribed non-patient care purposes and MOH's responses

Feedback	MOH's response
Respondents sought clarification on when NEHR data could be used for purposes beyond patient care.	There may be select instances where NEHR information may be shared for non-patient care purposes such as: (a) Public health purposes[2] approved by Minister (e.g. identifying affected patients in the event of a nationwide drug recall, so that they can be alerted to check their medications and consider seeking further medical attention) (b) Where it is permitted or required under other written law (e.g. for disease control and public health protection, including outbreak investigations and contact tracing of infected patients under the Infectious Diseases Act). Where NEHR information is shared for non-patient care purposes, only the minimum set of appropriate data required for the purpose will be shared with the relevant party (e.g. staff in the Health Sciences Authority for drug recall or MOH/CDA staff for contact tracing of infected patients). The recipient will also be required to delete or dispose of this information once the purpose for which it is shared is completed.

(D) Concerns surrounding medico-legal liability of healthcare professionals when accessing NEHR for patient care purposes

9. Some healthcare professionals raised concerns on the liability of a healthcare professional for unintentionally contributing inaccurate data to the NEHR, the obligations to access NEHR when treating a patient and the extent to which healthcare professionals must review all NEHR records when managing patients.

Table 4: Detailed feedback on the concerns surrounding medico-legal liability of healthcare professionals when accessing NEHR for patient care purposes and MOH's responses

Feedback	MOH's response
Healthcare professionals raised concerns surrounding increased medico-legal liabilities, even when accessing NEHR for care purposes.	*Contribution of health information to NEHR* Healthcare professionals should follow the Ethical Code and Ethical Guidelines (ECEG) on what constitutes a good medical record. This would include ensuring accuracy, clarity and contemporaneous records.

[2] This refers to any purposes that protects, improves or promotes the health and well-being of patients and communities in Singapore.

	Since specific segments of compatible HIMS are automatically contributed to NEHR, no additional step is required for healthcare professionals to ensure contemporaneous medical record contribution to NEHR. However, in situations where healthcare professionals become aware that there are technical issues which may delay the capturing of information into the HIMS or transmission of the information from HIMS to NEHR, healthcare professionals should ensure that the information is updated into the system as soon as reasonably possible. In the event of erroneous contribution to NEHR, enforcement will be calibrated. Generally, MOH will first work with the healthcare professionals to identify the cause of error and address it. Enforcement action will however be taken against Healthcare Providers who fail to meet contribution requirements despite repeated warnings. *Access to NEHR* The HIB does not change the ethical standards set out in the ECEG. Access to a patient's health record in NEHR is a supplementary tool for patient care, it does not replace or change clinical practices such as good history taking and the conduct of physical examinations. Healthcare professionals are encouraged to consider a range of factors before deciding whether NEHR access is required for a particular consultation such as: (a) Whether more information is required, based on the information gleaned from the history taking and physical examinations; or (b) Whether health records in NEHR would be relevant to the consultation. MOH will publish a set of guidelines on the appropriate use of NEHR information to address the medicolegal concerns of healthcare professionals in greater detail.

(E) Support measures to help Healthcare Providers transition and comply with HIB

10. Some healthcare professionals and smaller organisations highlighted compliance challenges with the HIB, including putting in place appropriate cybersecurity and data security safeguards.

Table 5: Detailed feedback on the Healthcare Providers' ability to meet their legal obligations under the HIB and MOH's responses

Feedback	**MOH's response**
Healthcare professionals and SMEs[3] raised concerns on the ability and readiness of smaller Healthcare Providers to meet the HIB requirements.	MOH acknowledges the concerns raised regarding smaller Healthcare Providers' readiness to meet HIB requirements. These requirements are essential to (1) ensure mandatory contribution to the National Electronic Health Record (NEHR) to enable safer, better and more connected care for all patients and (2) maintain robust cybersecurity and data security standards across our healthcare ecosystem to protect health data and safeguard the entire healthcare system MOH will continue with ongoing efforts to engage Healthcare Providers and support them in meeting various requirements under the HIB. This includes support measures, such as funding support, educational and training guides,

[3] Small and Medium-sized Enterprises.

	and training programmes. We have also published and will continue to maintain a whitelist of HIB-compliant health information management systems and qualified cybersecurity and data security service providers that Healthcare Providers could consider engaging. MOH is committed to supporting Healthcare Providers on this journey, including working with professional associations to achieve this.

11. During the public consultation exercise, MOH also received feedback requesting for greater clarity and clearer communication of the policy positions under the HIB.

Table 6: Detailed feedback for greater clarity and clearer communication of the policy positions and MOH's responses

Feedback	**MOH's response**
Respondents highlighted the need to continue communicating the HIB's policy positions clearly and transparently to stakeholders.	MOH will continue to enhance our website and public FAQs with the feedback obtained from the public consultation. MOH will also continue to engage stakeholders (e.g. Healthcare Providers and professionals) on the operationalisation of the HIB.

Conclusion

12. MOH would like to thank all respondents for their feedback.

13. Since the online public consultation, MOH has continued engagement sessions with relevant stakeholders. MOH remains committed to conducting further engagement sessions to support implementation of the HIB. We welcome the continued engagement with all stakeholders and interested parties.