

Home > Newsroom >

CLOSING SPEECH BY MR TAN KIAT HOW, SENIOR MINISTER OF STATE, MDDI & MOH, FOR THE...

Speeches

# CLOSING SPEECH BY MR TAN KIAT HOW, SENIOR MINISTER OF STATE, MDDI & MOH, FOR THE SECOND READING OF THE HEALTH INFORMATION BILL

12 January 2026

## Introduction

1. Mr Speaker, I thank all the Members who have spoken for supporting the Bill, especially our new NMP members – Ms Kuah and Dr Haresh – contributing to the debate on the first day they are sworn in. Sir, only by enabling data sharing and a unified health summary for each patient, can we support continuity of care when patients move between different healthcare settings and receive care from multiple healthcare providers
2. The Members have raised a number of thoughtful views and constructive comments, which I will address in four broad themes.
3. But before I do that, I will like to address the points made by Mr Kenneth Tiong, a Member, around the organisation and his views on Synapxe – the healthtech agency that implements many of the IT projects in MOH. As that topic does not pertain to the specifics of the Health Information Bill (HIB), I encourage Mr Tiong to raise a separate Parliamentary Question (PQ), or raise the issue separately from today's debate. But suffice to say that Synapxe is not a commercial entity. Its fundamental role is to support MOH in delivering digital health and IT services to benefit the healthcare clusters to deliver better services to our Singaporeans.
4. Let me now turn to the substance of the Bill. There are four broad themes of comments that came in.
  - a. First, around the **safeguards for patients**.
  - b. Second, the **obligations and support measures for healthcare providers**.
  - c. Third, the **support measures for healthcare professionals**.
  - d. And fourthly, the **sharing of non-NEHR health information**.

## Safeguards for Patients

5. Let me start with the safeguards for patients. Mr Yip Hon Weng, Mr David Hoe, Mr Wan Rizal, Dr Hamid Razak and Mr Fadli Fawzi highlighted the importance of safeguarding access to and use of patients' NEHR information.

6. And this has been a focus for us when we carried out the public consultation and prepared this Bill. There are broadly two sets of concerns that we hear from individuals.

- a. The first is how a patient's NEHR information will be adequately safeguarded and accessed only as needed by healthcare professionals and providers. Of special concern is the access to health information that may be deemed more sensitive. There



were also related questions about the Access Restriction feature. So that is the first set of concerns.

b. The second is around whether their NEHR information would be used beyond healthcare, such as for employment and insurance purposes.

### **Safeguards Governing Access to NEHR Information by Healthcare Providers**

7. Let me touch on the first set of concerns. Sir, we are not starting from scratch. We have been operating the NEHR for 15 years. Importantly, the vast majority of healthcare providers are already onboard – all public healthcare institutions, most private hospitals and the bulk of the General Practitioner (GP) clinics. So this is a system that is operating for many years.

8. And we have built in various ex-ante safeguards into the design of the NEHR. This includes role-based access, such that authorised healthcare professionals can only access the types of health information required for their specific patient care role.

9. We also have technical controls and regular ex-post audits to flag unauthorised accesses to the NEHR. With the HIB, we are enhancing the legislative safeguards and stiffening penalties for unauthorised access.

10. First time offences of unauthorised access of NEHR are punishable with a maximum fine of \$50,000 and/or up to 2 years' imprisonment upon conviction. And the penalty is doubled for repeat offenders. And healthcare professionals who access NEHR in an unauthorised manner could also be referred to the relevant Professional Boards or Councils for further action.

11. Mr Dennis Tan spoke about the offences and whether the \$1 million dollar maximum fine was sufficient. But sir, the jurisdiction he compared with as well as the Personal Data Protection Act (PDPA) that he referred to, do not have criminal prosecution. The breaches to HIB are serious, and we take this seriously. And for example, if you get convicted, it is not just fines, it is imprisonment as well. But more basically, we take an approach that is more supportive, working together with our healthcare providers and healthcare professionals. These are people – nurses, clinicians, administrators – who want to do well, serve the patients and take care of the patients. We want to take a supportive role and approach to uplift data security and cyber security postures, not the punitive approach.

### **Audits**

12. Mr Alex Yeo asked about audits on unauthorised accesses of the NEHR, and Mr Tiong asked if Synapxe would proactively monitor against unauthorised access. Synapxe, the NEHR system operator, conducts regular audits and ongoing monitoring to detect suspicious behaviour or atypical patterns, including in response to patient alerts.

13. For example, accessing the NEHR information of a patient who has not recently visited any healthcare provider is a flag. Synapxe will conduct investigations to determine whether an unauthorised access has occurred. Synapxe will regularly review its audit plans, including frequency, best practices and the use of new tools like Artificial Intelligence to ensure that the regime is robust.

### **Access Logs on HealthHub**

14. In addition, instances when a patient's NEHR information is accessed over the preceding 12 months will be made known to him through the "NEHR Access History" feature in the HealthHub application. This provides an additional layer of transparency.



15. Patients can monitor which healthcare providers have accessed their NEHR information and flag any unauthorised access to the authorities for investigation.

16. The logs will show access at the healthcare institution level to keep the function simple, usable and practical. In a multi-disciplinary team, healthcare professionals across different roles may access the patient's NEHR information at different times of the patient's care journey. Depending on the patient's condition, it is also not uncommon for nurses, pharmacists or allied health professionals to need access. In our healthcare system, the institution is ultimately responsible for care to its patients.

17. I would like to take the opportunity to clarify the comment made by Mr David Hoe. HealthHub access logs will show all access to the NEHR, regardless of whether they access it through the Electronic Medical Record (EMR) or the portal. So just to clarify on his point earlier.

18. Sir, I would like to assure Mr Hoe, Mr Fadli and Mr Yip that we will seek users' feedback when reviewing the interface to ensure it is simple and user friendly.

### **Health information that may be deemed more sensitive**

19. Mr Speaker, we understand that some patients are particularly concerned about access to health information that may be deemed more sensitive. Mr Louis Chua, Mr Yip, Dr Razak, Mr Hoe and Mr Tiong himself have commented on the need for safeguards for such information.

20. And such health information includes sexually transmitted infections, delusional disorders and schizophrenia. The diagnoses and test results that confirm the condition are subject to additional safeguards:

a. First, there are restrictions on who can access this information. Only a select group of healthcare professionals are allowed access to the information, based on their role in caring for the patient diagnosed with the health condition. For example, a nurse who is working in a psychiatric ward will have access to the psychiatric condition of the patient he or she is caring for. So that is the first control.

b. Second, before an authorised healthcare professional can access these types of health information, they will be subject to a double log-in, which requires the authorised healthcare professional to re-verify their credentials before access. This ensures such information is only accessed when needed and avoids accidental access.

c. Accesses to such health information are more closely audited by Synapxe, and cases of unauthorised access to NEHR information will be investigated and penalties imposed.

### **Patient Controls – Access Restrictions**

21. Sir, we appreciate that despite all these safeguards, some patients may still have privacy concerns. To assuage the concerns of these patients, the HIB will allow patients to restrict healthcare providers from accessing their NEHR information (or we call this "Access Restrictions" in the Bill). As I mentioned earlier in my opening speech, we do not encourage this as it could lead to adverse impact on care delivery for the patient.

22. So to address the queries raised by Members, Access Restrictions have been designed to balance the impact to patient care considering the welfare and interest of the patient, while taking into consideration their concerns around privacy.

a. So patients may restrict access to their NEHR information at the healthcare institution level, but not at an individual healthcare professional level. As I mentioned earlier, care delivery is team-based and increasingly multidisciplinary. It is not operationally feasible to restrict access to specific healthcare professionals but not others, when they all work in a team, in the same healthcare institution. This is aligned with good practices we observed elsewhere like in Australia.

b. Health information will be contributed to NEHR even if Access Restrictions are in place.



c. As pointed out by Dr Hamid, who brings in a practitioner's perspective, an incomplete record – including if individuals opt not to contribute select healthcare information deemed to be more sensitive – will significantly reduce the utility of NEHR in supporting healthcare professionals to provide quality care and could pose safety risks. In certain situations, access to such records in a timely manner could save lives, as I mentioned earlier in my opening speech.

d. One example will be when a doctor or pharmacist needs to have the ability to assess drug interactions, and his job is hindered due to incomplete medication information, the patient could suffer unintended consequences, especially in emergency situations when the patient may not be able to respond.

e. It also ensures that if patients change their minds in future, for instance, when they are older, and remove such Access Restrictions, there would be no gap in their NEHR information – and this was a valuable learning point when MOH colleagues engaged other jurisdictions.

f. The approach we are adopting aims to achieve a balance between patient choice and ensuring that patients receive better and more coordinated patient care.

23. Sir, in summary, healthcare providers would be granted access to NEHR to support patients' continuity of care across healthcare settings by default. Patients may, however, restrict access to all healthcare providers, or from second half of 2026, limit access so that only select healthcare providers, such as their own Healthier SG clinic, may access their information. Once in place, restricted healthcare providers will not be able to, unless required by other written laws, access the patients' NEHR information except for the essential subset of records that deals with allergies and vaccination records.

24. Next, I would like to also thank Members like Mr Yip, Mr Hoe, Mr Chua, Mr Fadli and Ms Kuah Boon Theng for highlighting the importance of educating the public on the implications of placing Access Restrictions and supporting patients that are less digitally savvy. We are likewise mindful of this point. MOH will work with the healthcare institutions to set up physical touchpoints for those who require help with placing Access Restrictions and understanding the implications of doing so. Alternatively, patients may seek the help of trusted individuals, like their family members and caregivers, to place Access Restrictions on their behalf.

25. Mr Yip raised the concern that the act of placing an Access Restriction may itself become a source of stigma or adverse inference. This Access Restriction will be known only to the healthcare providers managing the patient and all healthcare professionals are bound by their respective professional bodies' ethical codes and ethical guidelines to treat all patients fairly and without prejudice.

### **Prohibition from accessing NEHR for employment and insurance purposes**

26. Let me now move to queries around NEHR access for insurers and employers. We understand Singaporeans' concerns about the potential discrimination or stigmatisation they may face if their health information is revealed to their employer or insurer. On this, I would like to reiterate three points that I made earlier in my opening speech.

a. First, insurers and employers do not and will not have access to NEHR.

b. Second, healthcare professionals are also prohibited from accessing NEHR for employment or insurance purposes, except for prescribed statutory medical examinations which I will talk about later, or where authorised by other written law or order of the Court.

c. Third, the HIB imposes strict penalties for any unauthorised access to NEHR, with higher penalties for prohibited employment or insurance purposes.

27. Mr Wan Rizal asked whether statutory medical examinations may provide a backdoor for employers to gain access to NEHR information. The list of statutory medical examinations that is in the Bill is tightly scoped to those where NEHR access is necessary to protect the public and safeguard the health of the individual. This is the key principle.

28. We have no plans to expand this list to include employment-related screenings that are not necessary to protect the public and the individual. The current practice for employment-related screenings will remain – where doctors rely on their history-taking,



clinical assessment and their own existing medical records for the individual, if any, without access to NEHR.

29. On Mr Yeo's query on whether MOH would consider allowing individuals to give consent for their NEHR information to be accessed for insurance purposes for some situations, I would like to reiterate that NEHR is primarily for patient care purposes. When insurers request for health information, the current practice is for healthcare providers and professionals to rely on their medical records and patient interactions, which can include history-taking as well as physical examinations, to prepare the necessary reports for the insurer. This will continue to be the case after the HIB is enacted. NEHR must not be accessed for such insurance- and employment-related checks.

30. To Mr Tiong's query, healthcare providers and professionals should prepare separate medical reports, memos or clinical summaries for the insurer, instead of providing their raw medical records, such as print-outs from their clinical medical records. This is because raw medical records contain extensive information, including potentially irrelevant information. Where NEHR information is referred to during a medical examination, information relevant to the episode would be validated or confirmed with the patient during history-taking, and may be captured in the provider's own medical records together with the doctor's clinical assessment. Such information would then be treated as part of the provider's own medical records. Healthcare providers and professionals will need to carefully assess what information in their own medical records is relevant and necessary to include and report or provide to the insurer.

31. MOH has issued a circular to healthcare providers, and a guidance note to insurers, to clearly state this position. Healthcare providers may inform MOH if there are any inappropriate requests for NEHR information for insurance purposes.

### **Contribution of Health Information to NEHR**

32. Sir, let me now address questions about the contribution requirements in the Bill. Dr Haresh asked if mandatory contributions coupled with access would encourage episodic care, affecting initiatives such as Healthier SG, which encourages building a trusted relationship between patients and their family doctor. Mr Hoe asked about the requirement to contribute information in a timely and accurate manner and the treatment of such overseas medical records. And Mr Fadli Fawzi asked about the level of detail of key health information to be contributed to NEHR.

33. The Bill requires healthcare providers to contribute accurate and complete health information in a timely manner. This ultimately benefits patients by enabling their healthcare providers to access all relevant health information to provide the best care. Take a Healthier SG family doctor as an example: the Bill will allow the doctor to deliver better patient care, taking account of the patient's medical history across different settings including private specialist clinics. This enables the doctor to build a trusted and hopefully lifelong relationship, towards better health outcomes.

34. And to help healthcare providers comply with the contribution requirements in the Bill, we have whitelisted Health Information Management Systems (HIMS) that have the requisite technical features and encourage all healthcare providers to subscribe to these HIMS.

35. On overseas medical records, the HIB only applies within Singapore. Nevertheless, patients can bring their overseas health records to their local healthcare providers, who may then incorporate relevant information into their own medical records. And once incorporated, these records will be contributed to NEHR.

36. To Dr Hamid's query on whether populations that receive care outside the conventional system, such as prison inmates, would benefit from the Bill, I would like to reassure Members that all Singaporeans' key health information, including those under the care of the Singapore Prison Service, will be contributed to NEHR.



37. To Mr Fadli's query of NEHR's design to be a One Health Summary, we will only require the contribution of health information prescribed in the First Schedule of the Bill, and not the doctor's detailed clinical notes. The design of the system and the data pipes only take in the prescribed data types. For example, if a patient has diabetes and is prescribed insulin, the doctor will only need to contribute "diabetes" as the diagnosis, and "insulin" as medication. So only information that is needed for continuity of care.

### **Expansion of Scope of NEHR Information Sharing**

38. Sir, now let me turn to Dr Choo Pei Ling's suggestion to extend NEHR access to other users, such as allied health professionals working outside of licensed institutions.

39. I would like to thank Dr Choo for her suggestion to extend the access to other users. However, I would like to reiterate that the primary purpose of the NEHR is to support and enhance the continuity of care for patients. Hence, the HIB provides for NEHR access for licensed healthcare institutions. And within these healthcare institutions, NEHR access is only provided for healthcare professionals with clinical or care-planning roles. And this is the core principle governing NEHR access.

40. However, we recognise that as care models develop and evolve, we may need to grant new providers or services access to NEHR. In doing so, we will consider factors such as whether NEHR information is required for that role and whether the provider or service is able to comply with HIB's requirements. And prior to changing the scope of providers that may access NEHR, we will consult relevant stakeholders and publicly communicate the changes through the MOH website.

### **Sharing NEHR Information for non-patient care purposes**

41. Sir, Mr Chua, Mr Yip and Mr Fadli Fawzi also asked about the sharing of NEHR information for non-patient care purposes under the HIB, or other written law such as the Criminal Procedure Code 2010.

42. NEHR was set up to facilitate patient care, and the information within NEHR is primarily intended to be shared across healthcare providers for that purpose. And this is a consistent principle adopted by other jurisdictions that we have studied.

43. And MOH is of the view that identifiable health information should generally be interpreted and managed by qualified healthcare professionals. Parties from outside the healthcare sector generally do not require identifiable health information for non-healthcare-related purposes. Therefore, when parties seek MOH's views on this, MOH would suggest that such parties consider alternative data sources or ways of achieving its policy intent, instead of using NEHR information, or involve the qualified healthcare professionals to partner parties in meeting the intent.

44. For public health purposes under the HIB, NEHR information may be needed in certain situations, for example, to quickly identify and enable healthcare providers to contact affected patients in the event of a major drug contamination incident. Another example is in the event of an outbreak of a serious infectious disease. There may not be sufficient time, nor will it be feasible to seek consent from individuals to use their NEHR information to contain an outbreak. De-identified NEHR information may also be needed for public policy analysis and planning purposes such as to review healthcare utilisation trends or to analyse the cost-effectiveness of medicines.

45. I gave some examples to the queries that were raised by Members on the scenarios in which those clauses apply. As a general rule, MOH will ensure requests for NEHR information have sound basis before supporting them. For all requests, whether from private entities such as academic institutions and health-related organisations, or from public agencies under other written laws, MOH will share only the necessary data required to fulfil the intent.



46. Let me give another example to illustrate my point. For example, we received requests from the Police to locate missing persons. We only provide administrative information about visits to healthcare providers, without details of the patient's medical condition. This enables the Police to confirm if missing persons have been warded in an emergency, and in turn alert worried family members.

47. Requesting parties will also be required to protect the data against loss, and against unauthorised access, use, modification, disclosure or other misuse.

48. Mr Chua and Mr Fadli asked specifically about the use of NEHR for research. De-identifiable NEHR health information through established platforms such as TRUST under the National Research Foundation (NRF) for research purposes. These could include training for artificial intelligence models. But where requests are received from commercial parties, possibly for commercial purposes, we are extremely cautious in assessing such requests, including whether the sharing of such data is helpful in contributing to better healthcare and better health outcomes. Primarily NEHR is for continuity of care and for public health purposes, not for commercial purposes.

49. Mr Chua suggested allowing Access Restrictions to be applied to the sharing of NEHR information for broader public health interest purposes such as policy planning and analysis. This is not advisable, as it could lead to incomplete analysis and will undermine the utility of NEHR in informing national policies and planning.

### **NEHR – Resilience, Security and User Concerns**

50. Sir, now let me turn to the third topic around resilience and security of the system. A number of Members, including Mr Yip and Mr Dennis Tan, asked about the resilience and security standards for NEHR, particularly in light of the SingHealth data breach in 2018. I would like to reassure Members that MOH has taken in the recommendations under the Public Sector Data Security Review Committee conducted in 2019 and NEHR is complying with the relevant resilience and security requirements for government systems recommended by this committee.

51. NEHR is subject to security and resilience audits, with vulnerability scans, penetration tests and exercises carried out regularly to ensure that systems are secure and backup systems are operational in the event of a downtime. I must add that the lessons from the SingHealth data breach are that we are open and transparent about the issue, convened the Committee of Inquiry, learnt the lessons, applied them, and made sure we work very hard to prevent such breaches from reoccurring, and take those lessons to heart as we build up our cybersecurity and data security standards. And we have done so over the years.

52. Additionally, there are several lines of defence before the NEHR database, with intrusion detection at various parts of the network. Timely hardware, software and application upgrades are implemented, which include security patches, as well as security controls to detect and block suspicious traffic from external sources.

53. MOH and Synapse will continue to work with the Cyber Security Agency of Singapore, GovTech, and independent auditing firms to conduct regular cybersecurity reviews and security assessments.

54. I would also like to thank Mr Yip for his feedback on the need to make NEHR more user-friendly. I assure him that we will continue to invest in the improvement of NEHR's technology and features to help healthcare providers quickly identify the most relevant information for their patients.

### **Obligations and Support for Healthcare Providers**

#### **Cybersecurity and Incident Management Requirement**



55. Relatedly, Mr Yip, Dr Choo, Mr Hoe, Ms Joan Pereira and a number of Members like Mr Fadli Fawzi, Mr Tiong and Mr Dennis Tan, asked for further details on the cybersecurity and incident management requirements, including their feasibility and the availability of MOH support.

56. Sir, I would like to clarify that today, healthcare providers are already required to make reasonable security arrangements to protect personal health information. This is an existing requirement in laws such as the Personal Data Protection Act 2012 (PDPA) and Healthcare Services Act 2020 (HCSA).

57. The Bill's cybersecurity and data security requirements are based on these existing standards and legal requirements but contextualised for the healthcare sector. These include frameworks such as the Cyber Security Agency of Singapore's Cyber Essentials Mark (CEM), and the Infocomm Media Development Authority's Data Protection Essentials (DPE), which were designed to be accessible and implementable by smaller organisations.

58. And examples of these requirements include the use of anti-malware solutions and firewalls in computers, the backing up of essential business information and data storage practices. Healthcare providers will also need to train their staff on cyber-hygiene and data governance practices to ensure a safe and secure access to health information.

59. On the incident management framework, healthcare providers and their HIMS providers must put in place a framework to identify, resolve and mitigate cybersecurity and data breaches. This includes notifying MOH of prescribed security incidents and implementing mechanisms and processes to detect and respond to incidents such as ransomware attacks or unauthorised access to NEHR.

### **Safeguards for data breaches**

60. But even with the best preventive measures, a data breach may still occur. Healthcare providers will be required to notify MOH and affected individuals of significant data breaches. Once notified, MOH will work with the healthcare providers to understand the root cause of the breach, the extent of data exposed, the potential harm to patients and the containment and mitigation measures that need to be implemented.

61. In the event of any data breach, healthcare providers are expected to take necessary measures to remediate the situation and prevent such incidents from occurring again. Where MOH is of the view that the mitigation or preventive measures are inadequate, we will work with the healthcare providers on implementing the appropriate measures.

62. To Mr Fadli Fawzi's query on how "significant harm" will be defined, if a data breach causes or is likely to cause significant harm to an individual, for example if it involves disclosure of health information that may be deemed more sensitive, healthcare providers must notify the affected individuals upon or after notifying MOH. Additionally, MOH will only require significant breaches to be notified, in alignment with the approach under existing legal frameworks, such as the PDPA. These details will be set out in subsidiary legislation.

### **Support Measures for Healthcare Providers**

63. Let me now turn to the support measures for healthcare providers. I appreciate the concerns that Members have raised about the support needed for the smaller providers, especially smaller GP clinics. I mentioned earlier with Healthier SG, most GP clinics have already onboarded to NEHR with the support of MOH. MOH recognises the importance of providing healthcare providers with reasonable time to comply with the HIB requirements and will offer the necessary support for healthcare providers to prepare and adapt their systems and processes. We see them as a valuable partner in supporting the continuity of care in the community



64. And our support package will include measures to defray the costs of subscription to whitelisted HIB-compliant HIMS to digitalise their clinical records and to contribute data to NEHR more seamlessly. There are also other support packages to engage professional services from whitelisted service providers to implement cyber and data security requirements. Additionally, resources, guidance materials and training programmes will be available to help healthcare providers, including our community health partners, to meet the HIB cybersecurity and data protection requirements on an ongoing basis. We would like to reassure that providers that with this support in place, healthcare providers will be better enabled and supported to implement the relevant requirements.

65. We acknowledge the concerns raised by Mr Yip about potential fear-mongering tactics by some vendors. To address this, MOH is:

a. Developing basic service packages specifically tailored to the needs of solo practitioners and small and medium enterprises so that they can self-help, and prevent overselling of unnecessary services.

b. We are also establishing clear guidelines for whitelisted service providers on appropriate engagement practices and transparent pricing.

66. Healthcare providers that encounter unethical practices by whitelisted service providers can report them to MOH.

### **Specific Support for Pen-and-Paper Clinics**

67. Additionally, we recognise that there is a small group of what some Members call the “pen-and-paper” clinics that may face challenges in digitalising their clinics and meeting the Bill’s requirements. As Members highlighted, these clinics may require additional implementation support.

68. Sir, digitalisation is becoming key to the provision of healthcare. It is critical for clinical documentation, transmission of information between providers and laboratories, and supports timely coordination with other providers. Today, most clinics already have some form of IT system for clinic management, accounting and billing. Going forward, digital tools will increasingly become important, enabling clinics to rely on clinical decision support systems to close care gaps and deliver safer care.

69. Therefore, in recent years, we have strengthened the digitalisation in the private primary care sector to support Healthier SG and other national initiatives. Today, about 1,100 Healthier SG clinics are onboard suitable Clinic Management Systems and contribute to NEHR. Across the GP sector, more than 80% of them are on Clinic Management Systems. So there are a large number of clinics – a vast number of them already embarking on their digitalisation efforts. And we are supporting the remaining clinics to digitalise and onboard suitable systems to enable better delivery of care.

70. To Ms Joan Pereira’s query if smaller clinics could collaborate on shared resources, this is a good idea for smaller clinics to explore. Currently, clinics can already join the Primary Care Networks (or PCNs). PCNs not only provide peer leadership and support to small or solo GP practices, they also offer administrative assistance through the PCN headquarters. The PCNs will continue to offer advice and support to member clinics, share resources to smoothen clinics’ journey in digitalisation and fulfilling NEHR contribution. We will further consider Mr Dennis Tan’s and Ms Pereira’s suggestions on shared IT support services as part of the roll out.

71. I would like to assure Members that MOH is mindful of the administrative effort required to contribute information to NEHR. And this is why we encourage all healthcare providers to adopt a whitelisted HIMS which automates the process of contributing relevant health information to NEHR. That said, for smaller clinics that may require more time to digitalise, we will make available an alternative contribution channel so that these clinics will be able to start contributing data when required, while MOH continues to work with them on their digitalisation plans.



## Implementation and Enforcement Approach

72. Ms Kuah reflected concerns from the ground about time and effort needed for compliance, and if MOH will take these into consideration in event of non-compliance, especially in the initial period. MOH has worked closely with healthcare providers and professionals, and have been engaging them over the last few years. We have taken their feedback onboard:

- a. First, the Bill will commence in early 2027, to allow sufficient time for healthcare providers and professionals to familiarise themselves with the Bill's requirements.
- b. Second, to support their transition, guidance materials and dedicated support channels will be made available from the second quarter of this year to help providers and professionals understand their options and navigate the process.
- c. Third, should there be challenges complying with the Bill by the required timelines, MOH will consider the facts of each case carefully, and assist where appropriate.

## Support for Healthcare Professionals

73. Sir, now let me turn to the comments and suggestions for support for healthcare professionals. Dr Hamid Razak and Dr Choo enquired about how MOH intends to support healthcare professionals, noting that they have concerns about increased liability arising from the HIB. I think Dr Haresh also pointed out concerns from healthcare professionals on medical and legal liabilities and how they should think about it. We have been engaging the professional bodies and speaking to them for a period of time. And we have taken the suggestions, ideas and feedback on board.

74. MOH will publish a set of guidelines to support healthcare professionals' appropriate access and use of NEHR information. These guidelines will apply to not only the doctors but also to other healthcare professionals accessing NEHR, such as dentists, nurses and allied health professionals. Let me share some examples of the guidance that will be provided.

75. Healthcare professionals have asked whether they will be required to access NEHR for each consultation, and whether they need to review each record in NEHR when they do access it.

76. Accessing patients' NEHR information is not compulsory under the HIB. NEHR supports and complements existing clinical practices, including good history-taking and physical examinations.

77. HIB does not change existing standards and practices. Healthcare professionals are encouraged to consider a range of factors before deciding whether NEHR access is required for a particular consultation such as whether more information is required, based on the information gleaned from the history-taking and physical examinations; or whether health records in NEHR would be relevant to the particular consultation.

78. Sir, MOH will continue to work with the respective professional bodies to disseminate these guidelines to all healthcare professionals. We will also support professional bodies in ensuring their members' compliance with the Bill. On this note, I would like to take the opportunity to thank Ms Kuah for co-chairing the NEHR guidelines Workgroup Committee.

## Sharing non-NEHR Health Information to facilitate community-based care

79. Sir, let me now turn to health information that sits outside of the NEHR, and the clauses in the HIB that will enable the sharing of such information. Ms Pereira enquired about the timeline for enabling community health partners' sharing of such health information to be covered under the HIB. Mr Louis Chua asked why the HIB enables the sharing of non-NEHR health information without consent.



80. Today, the Agency for Integrated Care (AIC) shares data with community partners to enable them to engage and provide befriending services or care to seniors.

81. However, on the ground, there are difficulties with obtaining consent for data-sharing. Referencing my earlier example of Mr Lim, a 72-year-old gentleman who is managing his diabetes condition. He has stopped visiting his local polyclinic, and his polyclinic had faced difficulty in contacting him to obtain consent. The HIB will address this by providing an additional channel for the sharing of health information.

82. With the HIB, Mr Lim's polyclinic can potentially share his contact information and broad health risk indicators, such as an indication of the presence of frailty or chronic conditions, with AIC, without the details of specific medical conditions. AIC can then prioritise engaging Mr Lim to check on his well-being and link him with necessary support as needed.

83. On whether to include other community health partners like Active Ageing Centres and use cases in the future, MOH will carefully assess whether these other entities and use cases facilitate quality care and care continuity for patients.

a. We will consider their readiness to meet the various responsibilities that come with sharing health information, such as the cyber and data security requirements under the Bill. And we will consult key stakeholders.

b. Any community health partners which are added will be publicly communicated, including through MOH's website.

## Conclusion

84. Sir, to conclude, the HIB will help us achieve the goal of 'One Patient, One Health Summary, One Care Journey'. We will work with and support healthcare providers and healthcare professionals in achieving this goal.

85. Through our collective efforts, Singaporeans can benefit from better coordinated care, enhanced quality of care and lower costs.

86. Sir, I believe I have answered and addressed the questions raised by all the Members, and I beg to move.

[↑ Back to top](#)

## Ministry of Health

Staying healthy

Seeking healthcare

Ageing well

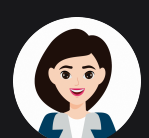
Managing expenses

Newsroom

Resources

About us


Reach us



[Contact](#)

[Feedback](#)

© 2026 Government of Singapore, last updated 7 May 2026

[Report Vulnerability](#) 

[Privacy Statement](#)

[Terms of Use](#)

[REACH](#) 

Made with



Built by

