HEALTH INFORMATION BILL 2024

Public Consultation – Policy Document

Ministry of Health, Singapore

Contents

Disclaimer

The information in this document is released for the purpose of public consultation only and does not represent or constitute the Ministry of Health ("MOH")'s final policy position(s) for the proposed legislation. MOH may continually review its policies and/or amend any information in this document without prior notice. Persons who may be in doubt about how the information in this document may affect them may seek independent legal or professional advice as they deem appropriate. MOH shall not be responsible or liable for any consequences (financial or otherwise), damage or loss suffered, directly or indirectly, by any person resulting or arising from the use of or reliance on any information in this document.

The Need for HIB

1. In our diverse healthcare system, most patients are seen and managed by more than one healthcare provider. The health information generated from each visit are held by these providers in separate paper or electronic record systems.

2. The system will likely become more diverse. Our healthcare system is continually evolving to meet the different demands of the population. By 2030, one in four Singaporeans would be aged 65 years or older. Demand for healthcare services will increase, and our healthcare needs will become more complex. More Singaporeans will have chronic conditions, will need to visit various healthcare institutions, and rely on multiple healthcare providers for care. With the greater adoption of remote healthcare technology, there is a rising demand for new services such as home care and telemedicine. Improvements in logistics systems also means that medications can now be delivered directly to one's home instead of only being available on-site at a doctor's clinic or a pharmacy.

3. Such increasing diversity in healthcare service delivery also means rising complexity in the flow of health information. Health information refers to any data that is about or related to an individual's physical and mental health, or the diagnosis, treatment, and care of the individual. In today's healthcare ecosystem, an enormous amount of health information is generated by healthcare providers each time they care for an individual. If we can share the key health information of patients, such as their vital signs, test results, medications, and allergies, it can facilitate more seamless and better care delivery.

4. This will benefit patients by removing the need for repetitive laboratory or radiological tests, and the need for patients to repeat their medical history to various healthcare providers. Very importantly, by having access to a common set of key health information of a patient, healthcare providers will be able to make better clinical decisions for the benefit of patients.

5. That is why the Ministry of Health (MOH) launched the National Electronic Health Record (NEHR), a centralised health information repository, which has been in operation since November 2011. NEHR makes available a longitudinal view of a patient's key health information to our healthcare providers, as a step towards achieving the vision of "One Patient, One Health Record". The NEHR serves to improve the flow of health information, by establishing a network between public and private providers. This allows patients to move seamlessly across the healthcare ecosystem to receive coordinated care regardless of setting.

6. However, while NEHR is used by all public healthcare institutions such as acute hospitals, community hospitals, and polyclinics, participation by private providers is voluntary, with about 15% participating so far, as of October 2023. Hence, differences in the systems used, and the level of IT adoption by healthcare providers means that while information is stored, it may not always be shared. Consequently, there is no

single holistic picture available of an individual's health information as data is fragmented and scattered across different providers.

7. Around the world, health authorities face the same challenge, and have been pushing for shared patient databases. In Singapore, having developed the NEHR system, the MOH is proposing to introduce the Health Information Bill (HIB) in the first half of 2024. The HIB will make it mandatory for all licensed healthcare providers to contribute data into the NEHR, and provide them access to patients' summary medical records for better care.

8. This will enable patients and providers to continue benefitting from having access to an up-to-date, accurate, and complete centralised national repository of key health information whenever care is provided. On the other hand, this also puts our healthcare system at increasing risk of cyber-attacks. The HIB therefore also proposes a robust unified set of cyber and data security requirements imposed on healthcare providers as they store and process health information. Finally, the HIB allows patients some flexibility to place access and sharing restrictions on their health information, without undermining our main objective for better care delivery. See Annex A for the full details relating to the proposed policies in the Bill.

9. MOH has consulted extensively on the proposed provisions of the HIB over the past year, with 39 focus group discussions conducted and over 1,000 stakeholders engaged. These include members of the public, our licensees, healthcare professionals and associations, as well as IT vendors, to design and refine the Bill. MOH is now further consulting the public and healthcare providers to seek feedback on the proposed policies in the Bill, as outlined within this document. Your feedback will help MOH to develop and implement robust policies for the Bill, and enable us to build a safer and secure digitalised healthcare system for everyone.

10. The public consultation will run from 11 December 2023 to 11 January 2024. Please submit your feedback at go.gov.sg/hib-consult-form no later than 11 January 2024, 6pm.

11. This document sets out the key provisions and issues under the HIB.

Key Provisions of the HIB

Contribution and Access of Key Health Information

12. For patients to continue benefitting from the NEHR, and for care transition to be made as seamless as possible across various providers, the NEHR must only contain accurate and up-to-date key health information of the patients, and be shared with the necessary healthcare providers.

13. The Bill will mandate all healthcare licensees to contribute a copy of selected key health information to the NEHR. MOH will be the approving authority in deciding which healthcare providers have to contribute to the NEHR.

14. The Bill will set out the types of information that healthcare providers must contribute, and the individuals which the requirement will apply (See Annex B)**.** For example, the health information of short-term visit pass (STVP) holders will not be required to be contributed as they are transient residents.

15. Only key health information will need to be contributed to the NEHR, as these are expected to be generally beneficial to all providers. This includes:

i. Patient Demographics (e.g., name, address, contact details);
ii. Visits (e.g., admission to a hospital, GP visit);
iii. Medical Diagnosis / Allergies;
iv. Operating Theatre Notes / Procedures / Treatments (e.g., endoscopy, surgical reports);
v. Discharge Summaries;
vi. Medications;
vii. Investigation Reports (e.g., laboratory reports such as blood tests, radiological investigation reports such as X-Ray Reports).

Such information is already being contributed to the NEHR by healthcare providers that are onboard the NEHR.

16. The process of contribution is intended to be automated. Providers using a compatible electronic medical record (EMR) system should not see a change in their practice nor any additional administrative burden when contributing data to NEHR.

17. All healthcare licensees will be granted access to the NEHR. Besides healthcare licensees, non-healthcare licensees may also be granted access as approved users, but they will have access only to the relevant information required for them to provide care to patients. For example, retail pharmacists may be granted access only to medication and allergy records so that they can flag out any unsafe interactions between medications that the patient is already consuming, with the other medications which the patient may be intending to purchase.

Sharing beyond the NEHR

18. The Bill will also set out three purposes for which health information residing outside the NEHR can be shared. These are (a) for outreach under national health initiatives; (b) to support continuity of care including telecollaboration; and (c) for assessment of eligibility for financing schemes. Administrative and clinical data may be shared for the purposes listed. For example, (a) for outreach – contact information; (b) for continuity of care – contact information and relevant clinical conditions; and (c) for assessment of eligibility of financing schemes – dwelling type. If care providers wish to share health information for purposes not provided for in the Bill, they will need to find a legal basis, for example, to obtain patients' explicit consent, or where provided for under other written laws.

Sensitive Health Information

19. While all health information is personal and sensitive, certain types of health information are even more sensitive, and risk subjecting individuals to discrimination or social stigma. The HIB terms such information as Sensitive Health Information (SHI). The list of SHI specified in Table 1 has been in place for some time and is currently defined under the Personal Data Protection (Notification of Data Breaches) Regulations 2021 for purposes of mandatory notification should there be a data breach.

20. SHI will not be readily accessible compared to other key health information. The intention is to mirror today's care environment, where all medical practitioners, selected nurses, and pharmacists, are granted access to patients' SHI. In public institutions such as a hospital, such access rights are granted based on their role in the care delivery of the patient. Nonetheless, granting access rights to professionals does not mean that the professional is allowed to access the SHI of patients that they are not providing care to or where such access is not required to deliver care for the patient.

21. Additional requirements will be imposed on such SHI. These include administrative access controls, such as a double log-in function within NEHR to ensure healthcare providers make a conscious decision when accessing such information, and mandatory incident reporting requirements should any breach of SHI occur. Furthermore, any unjustified use or access by unauthorised personnel will be subject to penalties.

Table 1: List of Sensitive Health Information

Sensitive Health Information	Specific Data Types / Examples
The assessment, diagnosis, treatment, prevention, or alleviation by a health professional of any of the following affecting an individual	

(a) any sexually transmitted disease, such as Chlamydial Genital Infection, Gonorrhoea and Syphilis.	• Chlamydial genital infection • Gonorrhoea • Syphilis
(b) Human Immunodeficiency Virus Infection.	• HIV
(c) schizophrenia or delusional disorder.	• Schizophrenia • Delusional disorder
(d) substance abuse and addiction, including drug addiction and alcoholism.	• Substance abuse (opioid abuse, inhalant abuse) • Substance addiction (drug addiction, alcoholism)
Any of the following: (a) subject to section 4(4)(b)* of the Act, the donation and removal of any organ from the body of the deceased individual for the purpose of its transplantation into the body of another individual; (b) the donation and removal of any specified organ from the individual, being a living organ donor, for the purpose of its transplantation into the body of another individual; the transplantation of any organ mentioned in paragraph (a) or (b) into the body of the individual.	• Organ donation and receipt (identity of organ donor, identity of organ recipient) • Transplant, transplant-related complications (e.g., liver transplant rejection)
The provision of treatment to an individual for or in respect of – (a) the donation or receipt of a human egg or human sperm; or	• Sperm donor • Sperm recipient • Egg donor • Egg recipient
(b) any contraceptive operation or procedure or abortion.	• Contraception operation or procedure • Abortion information
The suicide or attempted suicide of the individual.	• Suicide or attempted suicide
Domestic abuse, child abuse or sexual abuse involving or alleged to involve the individual.	• Domestic abuse, child abuse or sexual abuse

*Section 4(4)(b) of the PDPA – 4(4) This Act shall not apply in respect of - (b) personal data about a deceased individual, except that the provisions relating to the disclosure of personal data and section 24 (protection of personal data) shall apply in respect of personal data about an individual who has been dead for 10 years or fewer.

Personal Access via HealthHub

22. Individuals can monitor and track their own medical care and health plans, and individuals can continue to view information drawn from the NEHR within their HealthHub. As is the current practice, SHI will not be accessible via HealthHub. Parents of minors (aged below 21) will also continue to be able to view their child's HealthHub information, to better support their child in the management of their health

and well-being. Patients who require access to records on their SHI for any care purposes can still obtain the required information directly from their respective healthcare institutions, if it is not already in their possession.

Access for Non-Patient Care

23. In general, NEHR data should only be used for the provision of patient care and not for non-healthcare purposes. In particular, the HIB will explicitly disallow data to be used to assess one's suitability for employment, or to assess whether one can qualify to be an insurance policyholder or claimant, although insurance companies can continue to require medical check-ups as part of their under-writing process. This will ensure that a patient's medical history cannot be used to discriminate against the employability or insurability of the patient. This prohibition overrides patient consent to ensure that patients will not be coerced into giving consent for such assessments.

24. However, there are issues of public interest for which NEHR access may be required, even if they do not relate to patient care. They include the conduct of selected statutory medical examinations, which are examinations required by certain laws as a pre-requisite for the individual's participation in certain activities, to protect the individual's safety and welfare, and public interest. See Table 2 for examples.

Table 2: Use cases of statutory medical examinations for which NEHR access may be required

Fitness for role (e.g., to bear firearms, healthcare professionals)
Identification of persons with communicable diseases (e.g., Infectious Diseases Act)
Assessment of persons exposed to environmental hazards (e.g., Workplace Safety and Health Regulations)
Fitness for punishment (e.g., corporal punishment)
Assessment of residents/inmates upon admission (e.g., prisons)
Assessment of fitness to stand trial (e.g., Courts, Armed Forces)

25. The Bill will also allow MOH to approve requests for data to be extracted from the NEHR on a case-by-case basis. MOH will assess if it is in the interest of the public for such data to be provided to the requestor. One clear justified use is anonymised data for purposes of health research.

26. Individuals can check via HealthHub the NEHR access history (the date which a healthcare institution had accessed their records). They can request for MOH or Synapxe (as the NEHR system operator) to investigate potential cases of unauthorised access. Under the Bill, MOH will investigate cases where unauthorised access is suspected, and mete out penalties where appropriate.

Legal Concerns

27. Given the legal requirements surrounding the contribution, access, and use of NEHR, healthcare professionals have raised some concerns that they might inadvertently be taking on additional medico-legal liabilities once the Bill is implemented. To address these concerns, MOH has worked with a group of senior members of the medical, dental, and legal professions, and various professional associations, to draft a set of guidelines for healthcare professionals[1]. The aim of these guidelines is to outline the core ethical principles and reasonable professional standards that should be adopted when contributing to, accessing, or using NEHR**.** The guidelines will also provide additional information and guidance on the professional standards that all relevant healthcare professionals should continue to uphold, while using the NEHR as a tool to complement their professional practice. We welcome further feedback on the draft set of guidelines, and will incorporate relevant feedback in the final version, which is intended for launch around the same time as the introduction of the Bill in 2024.

28. Both medical practitioners and patients will need to work together to ensure that proper care can be delivered, since NEHR is meant to act as a complementary resource to assist in the clinical decision-making process. NEHR should not be viewed as a substitute to replace the doctor-patient relationship.

a. Medical practitioners will not be expected to access NEHR for every medical consultation. They should continue to exercise their professional judgement in deciding when to do so to supplement their clinical decision-making and maintain proper documentation of their medical records. Good history taking and physical examination are still fundamental requirements of care provision.

b. Patients should still take ownership of their own health and medical history by offering good history (to the best of their ability) when seeking medical attention. While doctors should and will run through patient's medical history to determine the best course of follow-up action, they are not obliged to review details if these are not assessed to be pertinent to the consultation at hand.

Access and Sharing Restrictions

29. The medical records of all individuals will have to be captured in NEHR under the HIB. Nevertheless, the Bill will provide individuals the option to place access restrictions on the sharing of their key health information in NEHR. Once in place, this restriction means that no one will be allowed to access the individual's information within the NEHR, including the individual's own attending doctor, and any statutory medical examination that the individual may be required to undergo.

30. As a result, the individual may experience more inefficient care delivery, leading to greater inconveniences to the individual, such as having to repeat laboratory or

[1] The draft Guidelines on Appropriate Use and Access of the National Electronic Health Record can be downloaded on the same REACH webpage as this document.

radiological investigations unnecessarily, and potentially even compromise their safety and welfare, as critical information, such as the individual's allergic reactions to medications etc., will no longer be made known to healthcare professionals. Similarly, caregivers will not be allowed to view the individual's HealthHub information if the individual has access restrictions in place.

31. Despite these protections for individual privacy, the Bill will allow for such access restrictions to be overridden in the case of a medical emergency, also known as a 'break glass' provision. For the 'break glass' override to be triggered, the individual must be (a) medically assessed to be at risk of immediate and significant harm unless medical intervention is given, and (b) unable to provide consent (e.g., because they are comatose). Access restrictions cannot be overridden for individuals who continue to have the ability to provide or withhold consent, even in a medical emergency. In such medical emergencies, only the medical practitioner and the supporting team attending to the patient will be allowed to view the NEHR information. NEHR access restrictions can also be overridden where required by other law, or when a court order is provided.

32. An individual who has placed access restrictions on their NEHR data will also be assumed to have restricted sharing of their health information residing outside the NEHR, and vice versa. However, it should be noted that the hospitals also access data through their internal electronic medical record systems, which are distinct from the NEHR which is a national health information system. Hence, notwithstanding that an individual can restrict access of key health information through the NEHR, doctors can still access data outside of NEHR, as part of their ethos and responsibility to provide the best possible care for the patient.

Cybersecurity and Data Security Safeguards

33. As custodians of the patients' healthcare data, healthcare providers contributing to or accessing NEHR, or care providers participating in data sharing use cases enabled under the Bill (collectively termed "entities"), will have to meet a unified set of cybersecurity and data security requirements to protect both electronic and non-electronic health information. These safeguards are necessary in view of the interconnected roles that healthcare and care providers play in the healthcare ecosystem. With an increase in the access, contribution, and sharing of health information across the ecosystem, there is a larger exposure surface to the threat of cyber-attacks and consequences of potential data losses.

34. The requirements build on the existing Healthcare Cybersecurity Essentials (HCSE) Guidelines, and are harmonised with other local cybersecurity and data security standards such as the Cyber Security Agency of Singapore (CSA) Cybersecurity Essentials, and the Infocomm Media Development Authority (IMDA) Data Protection Essentials. Full details of the requirements can be found in Annex C. For example:

a. Entities will have to ensure that their personnel undergo periodic cyber and data security awareness training.

b. If an entity engages a vendor to deliver a third-party system [e.g., a Clinical Management System (CMS) to support a GP's patient care], the entity must ensure that the system includes appropriate technical measures to protect the health information contained in the system. Such measures may include anti-malware scans, appropriate firewalls, and audit logs.

c. Under the Bill, the entity must also develop and implement processes to ensure that access to relevant patient health information is restricted and only accorded to personnel who need it for their work.

d. Finally, entities must establish a robust cyber and data incident response plan to clarify how they will detect and mitigate the impact of an incident, recover quickly, and ensure business-critical services can continue. This is so that patient care is not compromised.

35. MOH recognises that some smaller healthcare and community care providers may require additional support to adopt the requirements under the Bill. To help these providers manage compliance costs, MOH will review the need to develop grants and implement support schemes (e.g., training resources, funding support), as well as provide a whitelist of accredited vendors to ease transition. Further details on the implementation support will be announced subsequently. The list of existing digitalisation schemes is available in Annex D.

36. MOH will be surveying healthcare providers in the coming months, to better i) profile their IT set-up, resourcing, and capabilities, and ii) understand their current cyber and data security readiness. This will help inform subsequent steps that MOH may take to support healthcare providers in preparing for HIB's eventual implementation.

37. The Bill will require entities to report cybersecurity incidents and data breaches (including unauthorised access to the NEHR) that meet the prescribed thresholds[2] to MOH within 2 hours upon confirmation that the incident is notifiable. This allows MOH to take prompt action to limit the impact to patient safety and privacy, and detect early patterns that signal a larger-scale attack. For incidents affecting sensitive health information of a patient, entities are also required to inform the individual without undue delay.

Requirements for Data Intermediaries

38. Data intermediaries are organisations that process health information on behalf of an entity for purposes prescribed under the Bill, but do not include an employee of

[2] For example, a data breach is notifiable if it involves the health information of 500 or more individuals, or sensitive health information of any individual. More details are available in Annex A.

that entity. They include (but are not limited to) CMS vendors, IT service vendors, and data analytics platforms processing health information shared via the Bill. The Bill will impose obligations on data intermediaries, including (i) the protection of health information from unauthorised access or disclosure, (ii) the disposal of information that is no longer needed, (iii) ensuring data portability standards, and (iv) informing the entity of any cybersecurity incident or data breach without undue delay.

39. Even with these requirements, the entity is ultimately responsible for ensuring that the data intermediaries that it engages have sufficient safeguards to meet the HIB requirements. The entity's responsibilities include clearly defining the scope of work that the data intermediary will perform on its behalf, and for what specific purposes (e.g., a shared responsibility model) in the contractual agreements. This will help delineate accountability between the entity and data intermediary in the event of any non-compliances to the Bill.

Enforcement and Penalties

40. To ensure that all the requirements under the Bill are complied with and non-compliances dealt with in a timely and appropriate manner, MOH will have powers under the Bill to issue directions for entities to rectify non-compliances with the Bill, such as stopping unauthorised access to health information on the NEHR, destroying all health information collected in an unauthorised manner, stopping further unauthorised sharing of health information under the data sharing framework, and strict compliance with the cyber and data security requirements.

41. MOH will also have emergency powers to perform remediation measures involving health information in severe situations. These include directing the entity itself or for the entity to instruct other organisations or individuals to take action pertaining to the collection, transmission, modification, or destruction of health information. The powers can be invoked in any situation where the unauthorised processing of health information can cause serious and irreversible harm to patient safety (e.g., permanent disability and death), or serious disruption to healthcare service provision and capacity at the national level.

42. The penalty framework under the Bill aims to ensure that entities and individuals comply with the Bill and prevent unauthorised disclosure and misuse of health information. The penalties for non-compliance will be aligned to those in other relevant Acts. For example, penalties for an individual's unauthorised access to the NEHR, disclosure, and misuse of health information in the NEHR are proposed to be aligned with penalties in the Computer Misuse Act; and penalties for an organisation’s non-compliance to the cybersecurity and data security requirements are proposed to be minimally aligned with penalties in the Personal Data Protection Act.

43. For severe non-compliances by entities, MOH proposes to impose a fine of up to S$1 million, or 10% of the organisation's annual turnover (whichever is higher). Recognising the sensitivity of health information and to deter abuse, the Bill will also

introduce offences to hold individuals accountable for egregious mishandling of any health information under the control of an entity.

Conclusion

44. There is immense potential in having an up-to-date centralised record from which healthcare providers can draw upon to deliver seamless, informed, and appropriate care. The Bill further supports and enables the establishment of a safe, secure, and interconnected healthcare system, that prioritises patient safety and welfare. That said, MOH recognises that health information is personal to the individual and must be carefully and sensitively handled by those with access to the information.

45. MOH is seeking the views and concerns of members of the public, patients, healthcare providers, and data intermediaries whom this Bill will directly impact. Your comments will help MOH shape the Bill to address the needs of patients, and enhancing the quality and safety of the care delivered by our healthcare professionals in support of our national healthcare priorities and initiatives.