PROPOSED HEALTH INFORMATION BILL

FREQUENTLY ASKED QUESTIONS

Section One: The Need for the Health Information Bill

1. What is the Health Information Bill (HIB)?

- The HIB will govern the collection, access, use and sharing of selected health information in a safe and secure manner across various healthcare settings, to enable better continuity and transition of care and support outreach efforts.

- 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. 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. Sharing of health information also enables national healthcare initiatives such as Healthier SG and Age Well SG.

- The key provisions of the Bill are as follows:

    - Providers licensed under the Healthcare Services Act (HCSA Licensees) will be mandated to contribute selected health information to the National Electronic Health Record (NEHR). Approved contributors (non-HCSA licensees) such as retail pharmacists will also be mandated to contribute relevant information where generated.

    - Only HCSA licensees and approved users will be allowed to access health information in the NEHR for patient care purposes.

    - Beyond NEHR, sharing of non-NEHR data across the healthcare sector will be facilitated, amongst parties such as MOH, public healthcare institutions, and appointed private healthcare licensees as well as community partners.

    - There will be cybersecurity and data security safeguards put in place to govern the collection, access, use and sharing of health information.

2. Why do we need the HIB?

- As our population ages, demand for healthcare services will increase, and our healthcare needs will become more complex. More residents will have chronic

conditions, and need to visit various types of healthcare institutions, and rely on multiple healthcare providers for care.

- Such increasing diversity in healthcare service delivery also means rising complexity in the flow of health information. Today, the health information generated from each visit is generally held by each provider in separate paper or electronic record systems, which means it can be challenging for healthcare providers to have a single, holistic overview of an individual's health information.

- Sharing key health information of patients, such as their vital signs, test results, medications and allergies, across the many healthcare providers allows healthcare providers to make better clinical decisions and facilitates more seamless and better care delivery. Sharing of health information also enables national healthcare initiatives such as Healthier SG and Age Well SG.

- The HIB will further benefit patients by removing the need for repetitive laboratory or radiological tests, and the need for patients to recount their medical history to each of their different healthcare providers.

3. When is the HIB intended to come into effect?

- The HIB is intended to be read in Parliament in the first half of 2024. Mandatory contribution to NEHR will be rolled out in phases for the various healthcare providers, starting from end-2025, depending on the readiness of each category of healthcare provider.

4. What is Health Information?

- Health information is data relating to an individual's medical history which helps healthcare providers deliver informed care to the patient.

- Health information includes:

    - **Administrative data** which includes the patient's personal information such as name, address, contact details, as well as other demographic data. Such data is only considered as health information if used in relation to the provision, use or consumption of healthcare. Administrative data

could be used to assess eligibility for financial schemes and enhance the ability of community partners to reach out to targeted population segments to provide services, such as the befriender's programme.

- **Clinical data** which refers to all information about or in relation to (i) the physical and mental health of the patient, or (ii) the diagnosis, care, and treatment of the patient. This includes information such as prescriptions, investigation reports, procedures, and discharge summaries. Clinical data enables healthcare providers to holistically assess and treat patients. It is also used to ensure seamless care transition and follow up.

- Health information is usually found in:
  - The individual provider's hardcopy (paper) or electronic record systems; and.
  - The National Electronic Health Record (NEHR), a centralised repository of key health information, since 2011.

5. What is the National Electronic Health Record (NEHR)?

- NEHR is a centralised repository of heath information established in 2011 and is intended to serve as a source of selected key health information required to facilitate continuity of care across both public and private healthcare settings.
- 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. Consequently, for patients who use both public and private healthcare services, it may be challenging for healthcare providers to have a holistic overview of these patients' health information.

6. What is the purpose of the National Electronic Health Record (NEHR)?

- NEHR is developed to facilitate data sharing between healthcare providers and allow for better care coordination, as patients receive care from multiple care settings.

- For healthcare professionals, NEHR provides greater visibility of the patient's medical history and test results. This allows the healthcare providers to be better aware of his patient's overall condition and to make better care decisions for his patient.

- For patients, beyond experiencing better care provision, it is expected that there will be reduced need for repetitive laboratory or radiological tests, or for patients to repeat their medical history to each of their different healthcare providers.

7. Is this MOH's first consultation on the HIB?

- MOH has consulted extensively on the proposed policies 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 policies.

- MOH is now further consulting the public, healthcare providers and IT vendors to seek feedback on the proposed policies in the Bill.

Section Two: Contribution and Access of Key Health Information

Contribution to NEHR
8. Who needs to contribute to the NEHR under the HIB?
• Under the HIB, all HCSA licensees must contribute selected key health information to the NEHR. MOH may also approve non-HCSA licensees ("approved contributors") to contribute relevant information to the NEHR. • Approved contributors are organisations (other than HCSA licensees) which provide some form of patient care, and hence are expected to generate data which is useful to be stored in the NEHR to support continuity of care across healthcare institutions. Retail pharmacies are an example of organisations that may be approved as approved contributors. • You may refer to www.hcsa.sg for a list of the categories of licensees under the HCSA. MOH will also publish a list of any approved contributors.
9. Must all licensees and approved contributors contribute the same set of key health information to the NEHR under the HIB?
• As part of the HIB, HCSA licensees will be mandated to contribute key health information to NEHR to support continuity of care across healthcare institutions. • The HIB will set out the types of key health information that each category of HCSA licensee must contribute, based on the type of patient care provided and health information generated. • Approved contributors will need to contribute information that has been included as part of their approval conditions. • Notwithstanding this, the Bill will only require contribution of health information where such information is generated. For example, if a GP does not prescribe medication to a patient he sees, he will not need to contribute information on prescriptions to the NEHR for that visit.

10. What information will be mandated for contribution to the NEHR?

- Only key health information useful for continuity of care will be mandated for contribution. This includes:
    - Patient Demographics (e.g., name, address, contact details)
    - Visits (e.g., admission to a hospital, GP visit)
    - Medical Diagnosis / Allergies
    - Operating Theatre Notes / Procedures / Treatments (e.g., endoscopy, surgical reports)
    - Discharge Summaries
    - Medications
    - Investigation Reports (e.g., laboratory reports such as blood tests, radiological investigation reports such as X-Ray Reports)
- Detailed information which resides in the healthcare providers' medical records, such as day-to-day progress and clinical notes, would not be contributed to the NEHR. Such granularity may not be equally beneficial nor applicable for providers in the various care settings and make the NEHR difficult to navigate.

11. Will contributing data to the NEHR result in additional work for healthcare providers?

- Providers using a compatible electronic medical record (EMR) system should not experience any change in their practice or additional administrative work when contributing data to NEHR.
- A compatible EMR system will allow selected data fields to be sent to the NEHR automatically, with no need for the healthcare provider to manually update the data fields in NEHR.
- MOH encourages all healthcare providers to digitalise and adopt solutions which are NEHR-compatible to avoid any unnecessary workload for the contribution.

12. When will mandatory contribution for the NEHR be implemented?

- Should the HIB be passed, MOH intends to implement mandatory contribution in phases, starting from end-2025, depending on the readiness of each category of healthcare provider. This is to allow sufficient time for HCSA licensees and approved contributors to meet the requirements stipulated in the Bill.

13. How are HCSA licensees being encouraged and assisted in accessing / contributing to NEHR?

- MOH has made available several types of support (e.g., funding, clinical informatics) to incentivise HCSA licensees to contribute to the NEHR earlier.

- For instance, the Early Contribution Incentive (ECI) scheme is a one-time funding support designed to help private HCSA licensees defray the cost of upgrading and/or integrating their IT systems with the NEHR. The GP IT Enablement Grant is a one-off grant to support GP clinics in digitalisation and to adopt a suitable Clinic Management System (CMS) under the CMS Tiering Framework for Primary Care which covers contribution to NEHR.

- MOH (through Synapxe) will provide training and support to HCSA licensees as part of their onboarding process, to ensure licensees know how to configure their system to submit data in the required format. These include conducting workshops and providing mapping services for the Singapore Drug Dictionary (SDD). More information can be found at the following link.

- MOH will also conduct a survey to better understand the current cyber and data security maturity levels of providers, including digitalisation levels, to better assess the nature and type of support required. This will complement efforts to better understand licensees' ability and readiness to contribute data to NEHR. Existing outreach efforts by Synapxe will continue, to help licensees better understand the benefits and use of NEHR.

Access to NEHR
14. Who can access NEHR data?
• In general, only care providers (which includes all HCSA licensees as well as selected non-licensed healthcare providers) who are directly caring for a patient may access that patient's NEHR, if NEHR information is relevant for patient care. Providers should not access NEHR when the patient is not directly under their care. • Selected non-licensed healthcare providers may be granted access as approved users but can only access information required for their role. For example, retail pharmacists may be granted access to medication and allergy records so that they can flag out any unsafe interactions between medications that the patient is already consuming and other medications the patient intends to purchase. • The non-exhaustive list of scenarios below illustrates some of MOH's views on NEHR access. Further guidance is available on the Draft Guidelines on Appropriate Use and Access to the National Electronic Health Record, which can be found at the same REACH website where the public consultation is held (go.gov.sg/hib-consult). • Scenario 1: Even if requested, a doctor cannot access the NEHR data of their family member, if the family member is not registered as a patient under the doctor's care. NEHR access is appropriate if the family member is registered as a patient under the doctor's care. • Scenario 2: If a doctor is asked by a colleague for an informal opinion on a patient, and the doctor does not have a care relationship with that patient, it is not appropriate for the doctor to access that patient's information on NEHR. However, it is reasonable for a doctor to access NEHR to prepare for the first consultation with a referral patient after pre-registering the patient and setting an appointment date. The creation of an appointment for the patient indicates the beginning of the care relationship, albeit a limited one, which justifies the use of NEHR.

- Scenario 3: It may be appropriate for a clinic to grant its nurse access to NEHR if the nurse was employed or engaged by the clinic to provide patient care, and the nurse needs to consult NEHR to discharge such patient care responsibilities. However, it would not be appropriate to grant NEHR access to a staff engaged purely for administrative work that is not involved in direct patient care. Ultimately, which individuals are granted access will depend on the roles that they play within each individual institution.

15. What are the user controls to protect against unauthorised access?

- NEHR users should only access NEHR for direct patient care or for uses that have been approved by MOH.

- Each clinic or institution needs to authorise different types of users (e.g., doctor vs. pharmacist), depending on the roles they play within the institution. The system only displays information allowed for each type of user. The NEHR System Operator regularly reviews whether the information each user type can access is appropriate for their role. Measures are also in place to detect suspicious or unusual patterns of NEHR access, which will be audited, with enforcement action taken against unauthorised access of NEHR.

- Additional controls are in place for NEHR administrators, where their access is on a "need-to-use" basis and, like banks, have two layers of security (e.g., username & password as well as authentication via the banking app) when logging in. These administrators' activities are logged and analysed for unusual activities.

16. How can members of the public check accesses to their NEHR data?

- The NEHR Access History feature has been made available on HealthHub since Nov 2021. This enables patients to view a log of accesses made to their own NEHR records (by date and healthcare institution) and report any suspicious or suspected wrongful access.

- When suspicious access is reported, investigations will be carried out accordingly and actions will be taken against unauthorised access of NEHR.

Use of NEHR data

17. What can individually identifiable NEHR data be used for?

- Individually identifiable NEHR data is to be used for the following purposes:
    - Direct patient care purposes, which include:
        - Provision of a healthcare service to an individual;
        - Any administrative matter directly related to the provision of the healthcare service to the individual, such as admissions and discharge relating to the care provider, scheduling of the individual's appointments with the care provider, and transfer or referral of the individual to another care provider who may provide a healthcare service to the individual.
    - Where required by law (for example where required under the Criminal Procedure Code or a court order, or as part of a designated list of statutory medical examination, such as those required to assess an individual's fitness for a role in the uniformed services).

18. What are the statutory medical examinations for which will MOH allow NEHR data to be used?

- MOH is considering allowing use of NEHR data for these statutory medical examinations:
    - 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)

- Nonetheless, to continue upholding patient autonomy, medical practitioners will still not be able to access the NEHR of individuals who have placed access restrictions on their records, unless such individuals lift said restrictions.

19. Can NEHR data be used for research or publication?

- Being granted access to NEHR data does not permit a healthcare professional to use any NEHR data, whether of their own patients or colleagues' patients, for clinical research or publication. This applies to anonymised or aggregated data, and even where patients have consented to the use of NEHR data for research or publication.

- Healthcare professionals who wish to use NEHR data for any form of research or publication should seek specific approval from MOH.

- MOH takes a serious view of any unauthorised access and use of NEHR data. Such cases will be investigated, and action will be taken against the errant users accordingly.

Security of the NEHR

20. Should mandatory contribution to the NEHR still be considered, given that patient data could be at risk in a cyberattack?

- Technology remains a key enabler for the delivery of effective and efficient healthcare for Singaporeans. The NEHR is an important national system that will bring about significant benefits including safer patient care and better continuity of care across various clinical settings in the public and private sector.

- We also recognise the increasing cybersecurity threat and will continue to fortify our defences to safeguard our electronic systems and protect patient data.

- MOH has assessed that, on balance, the benefits to patients and providers from mandatory contribution to NEHR and continued access to an up-to-date, accurate and complete centralised national repository of key health information outweigh the risk posed by cyber-attacks.

21. What would happen if there were a major security breach of NEHR? What steps would MOH take to stop the unauthorised circulation and disclosure of personal health information?

- In the event of a major security breach, immediate action will be taken by MOH and the System Operator, Synapxe, to secure the NEHR system and stop further unauthorised circulation and disclosure of personal health information.
- This includes promptly investigating the incident and conducting digital forensics and analysis to identify the exposure and the root cause(s) of the breach.
- Should any data be exposed to the public over internet websites, legal take-down notices will be sent to the websites' registered owners to lock-down such personal data and prevent further circulation.
    - Affected patients will also be notified in line with the prevailing personal data regulations.

22. What is the status of the security reviews for NEHR?

- The NEHR has been subjected to a series of cybersecurity reviews conducted by the Cyber Security Agency of Singapore, GovTech, and independent auditing firms.
    - These cover technical architecture design and existing cybersecurity measures.
    - A series of infrastructure vulnerability scans and application penetration tests were also conducted to uncover any security vulnerabilities against cyberattacks.

- MOH and Synapxe have reviewed the findings from the cybersecurity assessments and have implemented enhancements to address the findings.

23. What changes have been made to improve the security of NEHR and protect NEHR against cyberattacks since the SingHealth cyberattack?

- There are several lines of defence before the NEHR database, with intrusion detection at each line. Timely hardware, software and application upgrades are implemented, which include security patches, as well as applications to detect and block suspected malicious traffic from external sources. Regular security audits, vulnerability scans and penetration tests are also being conducted.

- MOH and Synapxe will continue to work with Cyber Security Agency of Singapore, GovTech, and independent auditing firms to conduct regular cybersecurity reviews and security assessments on the NEHR to strengthen the security posture of the system.

- MOH and Synapxe also collaborated with GovTech in crowdsourced vulnerability discovery programmes; namely Vulnerability Rewards Programme (VRP), Government Bug Bounty Programme (GBBP) and Vulnerability Disclosure Program (VDP). This is to encourage the cybersecurity community and public through proactive identification and remediation of vulnerabilities to strengthen the security posture of NEHR system.

24. When was the last time a cybersecurity audit was done on the NEHR system?

- Besides the audits conducted by the Cyber Security Agency of Singapore, GovTech, and independent firms, Synapxe conducts other internal security tests, assessments, and maintenance on the NEHR systems. These include penetration tests and vulnerability scans.

- The last penetration test and vulnerability scan were conducted in November 2023.

25. How are unauthorised accesses of NEHR detected?
• Synapxe has implemented measures to detect suspicious/unusual access to NEHR. When unusual user access is detected, the relevant healthcare institution will be alerted to investigate the case. Confirmed cases of breaches will then be reported to MOH for enforcement action. • Disciplinary and/or enforcement actions may be taken against users who inappropriately access or use NEHR, based on the severity of the breach.

Section Three: Sharing beyond the NEHR

Data Sharing
26. Other than NEHR, can my health information residing in other systems or records be shared across healthcare providers for patient care, under the HIB?
• To ensure continuity of care, MOH is planning to allow sharing of non-NEHR data for specific purposes. The Bill will prescribe (i) the purposes for which data can be shared, (ii) the care providers which can perform such sharing or receiving of data, and (iii) the types of data that can be shared. All three criteria must be fulfilled for the data sharing to take place. • The Bill will 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 – housing type. • If care providers wish to share health information for purposes not provided in the Bill, they will need to find a separate legal basis, for example, by obtaining patients' consent, or where provided for under other laws.
27. Who can share and receive my non-NEHR health information?
• The purpose, provider, and dataset for any sharing of non-NEHR health information will be prescribed in the Bill. For example, sharing of contact information and relevant clinical information between two general practitioners (GP) for continuity of care purposes, where a patient may decide to switch GP after moving house. • Care providers (both sharing and receiving) must meet the requirements stipulated within the Bill (for example, having the receiving entity's confirmation

that it has met the appropriate cyber and data security requirements) before they engage in data sharing.

- Not all individuals employed or engaged by the care providers can share or receive health information. The Bill will also prohibit the unauthorised access, use and disclosure of health information by unauthorised persons (i.e., persons that have not been authorised by the healthcare provider or prescribed in the Bill to be able to access, use or disclose data).

- Any onward sharing of any such data without the individual's consent will be investigated and met with the appropriate penalties under the Bill.

28. Why are new provisions on data sharing required under HIB? Isn't NEHR sufficient for continuity of care?

- While NEHR has a copy of key health information which can be used to support continuity of care, NEHR access is strictly protected for patient care purposes. Other health-related systems beyond the NEHR may also contain health information that can be used to benefit patients.

- These include more detailed care notes that each care provider would have kept a record of in their delivery of care to the patient. Such granularity may not be captured by the NEHR. Not all care providers (especially community care providers) have access to the NEHR as well. Such providers would require a means to obtain health information from other providers, so that they may provide appropriate care to the patient.

- For example, a social worker in a social service agency (SSA) may not have access to the NEHR and will have to depend on the referring hospital to provide them with adequate information to make an assessment on the patient's eligibility for a financing scheme.

- Nonetheless, MOH is aware that the data sharing landscape is complex today due to the fragmented nature of health information. The Bill will simplify the health data sharing framework. This will help facilitate the flow of information between providers and benefit patients in care delivery.

29. Why is there a need to share data with our community partners?

- Shifting care beyond hospital to the community is increasingly important in care delivery. For example, with Healthier SG, our community partners (e.g., Active Ageing Centres, Health Promotion Board, SportSG) are an integral pillar of our shift towards preventive care and care closer to home, as they oversee various community care services, and run a range of healthy lifestyle activities and programmes in the community. Your enrolled family clinic will also tap on them to support you for some basic care needs and leading healthier lifestyles.

- Unlike a traditional illness where doctors may refer you to a specialist, in a preventive care plan, the family doctor may refer you to healthy lifestyle programmes in the community that are run by partners, such as Health Promotion Board and SportSG, to attend an exercise programme.

- These community partners would thus need access to up-to-date data to reach out to residents accordingly and guide them to relevant services. As such, MOH intends to permit approved entities to share permitted types of data residing outside the NEHR for prescribed purposes under the HIB. This will enhance our whole of community support to help Singaporeans detect illness early and manage chronic diseases well.

30. What are the safeguards in place to ensure data is securely shared under the HIB?

- The HIB will put in place specific data governance and security requirements for healthcare providers. Some examples include:

    - Requiring residents' health data to be properly managed and accessed only on a need-to-know basis.

    - Ensuring that health records are always kept confidential, and that measures are in place to govern the appropriate use, disclosure and retention of such data.

    - Putting in place strict cyber and data security measures to ensure data is secured.

- An appropriate enforcement and penalty framework will also be put in place so that necessary actions can be taken against providers when safeguards are not met or adhered to (e.g., unauthorised or inappropriate access or use of data).

Section Four: Sensitive Health Information

31. What is "Sensitive Health Information"?

- Sensitive Health Information (SHI) refers to health information that could lead to severe, long-lasting stigmatisation or discrimination and requires additional safeguards to prevent any unauthorised access and use. The list includes the following:
    - Sexually transmitted infections, HIV Infection (i.e., HIV, chlamydial genital infection, gonorrhoea, syphilis)
    - Mental Disorders (i.e., schizophrenia, delusional disorder)
    - Substance Abuse & Addictions (e.g., drug addiction and alcoholism)
    - Biological Parenthood (i.e., sperm donor, sperm recipient, egg donor, egg recipient)
    - Voluntary Sterilization; and Termination of Pregnancy (i.e., contraception operation or procedure, abortion information)
    - Organ donation (i.e., Identity of donor, identity of organ receiver, transplant)
    - Suicide (i.e., suicide or attempted suicide)
    - Abuse (i.e., domestic abuse, child abuse or sexual abuse)
- The HIB will mandate entities to report data breaches to MOH and inform affected individuals without undue delay if there are any suspected breaches of SHI.

32. Will Sensitive Health Information be contributed to the NEHR, and who can access it?

- Sensitive Health Information (SHI) will be contributed to the NEHR, as it forms a critical part of patients' medical history.

- To protect patient's privacy, only authorised healthcare professionals, e.g., doctors, selected nurses and pharmacists, are allowed to access SHI as they may require this information to make proper decisions on the treatment and management regarding the patient.

- All authorised healthcare professionals with access to SHI are required to respect the confidentiality of their patients and are expected to safeguard such information.

- Further, receiving access rights to SHI does not mean that authorised healthcare professionals are 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.

- Beyond access to SHI being restricted to authorised healthcare professionals, SHI in NEHR is protected by a "double login" feature (i.e., authorised healthcare professionals accessing the Sensitive Health Information are required to consciously re-login and provide reasons for access before the information is shown to them). All accesses are tracked.

33. Can access to all sensitive health information in NEHR be blocked when clinical data are shared among providers?

- While we are aware that unauthorised disclosure of sensitive health information could lead to severe, long-lasting stigmatisation or discrimination, we do not support blocking access to these records as it will limit the use of NEHR and result in gaps in patient information, thereby affecting the clinical care provided to patients.

- To safeguard the access and sharing of Sensitive Health Information, we have put in place additional controls to restrict its access (such as a "double login" feature, and only granting access to relevant healthcare professionals).

- Further, the HIB will mandate entities to report all data breaches to MOH and inform affected individuals without undue delay if sensitive health information is

affected. We will also take appropriate enforcement action against those who misuse their access to SHI.

- An individual can also place access restrictions on his NEHR records, which will prevent any provider from accessing his NEHR data. However, if an individual restricts access to their NEHR records,
    - All healthcare professionals, even those that are providing care to the individual, will not be able to access the individual's NEHR records, which may affect care provision.
    - The individual may not be able to participate in national programmes such as Healthier SG that require sharing of health information to allow continuity of care.

Section Five: Personal Access via HealthHub

34. Will HealthHub, Healthy 365 and NEHR be integrated?
• Today, HealthHub and NEHR are already integrated. Certain relevant health information submitted to NEHR such as prescriptions, selected laboratory results, screenings and discharge summaries are viewable by patients and authorised caregivers via HealthHub. They can also perform self-service transactions, such as booking medical appointments, via HealthHub. • Healthy 365 is a separate mobile application focusing on daily interactive lifestyle engagements such as lifestyle activities tracking, health programme recommendations, and nudging and rewards management to influence the adoption of healthy lifestyle behaviours and habits. GPs can use information on Healthy 365 as part of the holistic care provided to enrolled patients under Healthier SG.
35. What information from NEHR can be viewed on HealthHub today?
• All individuals will continue to be able to view information drawn from the NEHR through their HealthHub accounts. This is to allow individuals to monitor and track their own medical care and health plans. • Parents and caregivers will continue to be able to respectively view their child's (aged below 21) and dependent's HealthHub information using their own HealthHub account. • Like today, Sensitive Health Information (SHI) will not be displayed on HealthHub to maintain the security of these sensitive information and prevent inadvertent leakage. Individuals who require their SHI for any care purposes can approach their respective healthcare institutions, if it is not already in their possession. • Information from NEHR which can be viewed via the HealthHub app or portal include: 1) Medication / Immunisations.

2) Selected Investigation Reports (general laboratory results, chest x-rays, mammograms)

3) Inpatient discharge summary

~~4)~~ NEHR Access History

Section Six: Access for Non-Patient Care

36. Can employers and insurers access NEHR data when assessing an individual's suitability for employment or insurability?
• Employers and insurers are NOT given access to NEHR. Only healthcare providers are given access to NEHR. • Access to the NEHR is intended for direct patient care purposes. Healthcare providers engaged by employers or insurers are not allowed to access the NEHR to obtain information to assess an individual's suitability for employment or insurance, even with the patient's consent, unless the access is required by any law or a court order.
37. If a healthcare provider is also an insurance third-party administrator (TPA), how does MOH ensure that NEHR information is not passed from the healthcare provider to the insurance TPA and subsequently the insurer?
• Healthcare providers are not allowed to access NEHR for employment or insurance purposes. They are also not allowed to disclose such information to those not participating in the care of patients. They are only allowed to use information that is already existing in their own medical records.
38. Why are patients not allowed to give consent for a doctor to access their NEHR data for employment or insurance purposes?
• Healthcare providers engaged by insurers or employers are not allowed to access the NEHR to obtain information to assess an individual's insurability or suitability for employment even with patient consent unless this is required by any law or a court order. • This is to ensure that a patient's medical history (e.g., history of schizophrenia) is not used to discriminate against employability/insurability of the patient, and that patients are not pressured into giving consent for such purposes. • Users who are found to have accessed the NEHR for such prohibited purposes may be subject to a fine, imprisonment, or both.

Section Seven: Medico-Legal Issues

39. How does MOH intend to address the medico-legal issues on NEHR that healthcare professionals raised?

- During previous consultations on the policies of the HIB, some healthcare professionals raised 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 profession and various professional associations to draft a set of guidelines for healthcare professionals.

- 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.

- The guidelines are planned for issuance around the same time as the introduction of the Bill in 2024. A draft of the guidelines can be found at the same REACH webpage on the public consultation (go.gov.sg/hib-consult).

40. Does a patient withholding consent mean that a healthcare professional does not contribute the patient's health information to NEHR?

- Under the HIB, it will be mandatory for all HCSA licensees to contribute a copy of their patients' selected key health information to the NEHR.

- When connected to the NEHR, the default is for the practices' and institutions' electronic records system to automatically send a copy of all patients' selected key health information from the practice's and institution's electronic records system into NEHR. However, detailed information which resides in the healthcare providers' medical records, such as day-to-day progress and clinical notes, would not be contributed to the NEHR.

- Patients may choose to restrict all care providers' access to their health information in NEHR. However, restricting access does not prevent the patient's selected key health information from being automatically contributed to NEHR. This is to prevent any gaps in the patient's records should the patient choose to allow access to their NEHR data in the future, such as during medical emergencies.

41. Must a healthcare professional access and use health information on NEHR for every consultation?

- Healthcare professionals are not expected to consult NEHR at every single clinical encounter. When they decide to do so, they are not expected to review every single past medical record.

- In addition to taking guidance from relevant professional codes, such as the Singapore Medical Council's (SMC) Ethical Code and Ethical Guidelines (ECEG), healthcare professionals can refer to the factors listed below when considering when to consult NEHR for the purposes of patient care.

- Factors to consider when deciding if it is reasonable to consult NEHR include:

    - Whether history-taking and physical examination was sufficient for a reliable clinical assessment;

    - Whether more information is required;

    - Whether information in NEHR would be relevant to the current consultation.

42. Does mandatory contribution to NEHR and hence the increased amount of information on NEHR mean that healthcare professionals are fully responsible for ensuring good outcomes?

- Both medical practitioners and patients will need to continue to work together to ensure that proper care can be delivered. NEHR is a complementary resource to assist in the clinical decision-making process and is not a substitute for the doctor-patient relationship.

- For healthcare professionals, history-taking and physical examination remain the mainstay in clinical assessment. NEHR is an additional tool that can complement and aid clinical assessment. Healthcare professionals are not expected to consult NEHR for every clinical encounter.

- Patients should still take ownership of their own health and health information 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 access the NEHR if the information there is assessed as not pertinent to the consultation at hand.

Section Eight: Access and Sharing Restrictions

43. Can an individual prevent their own data from being contributed to NEHR?

- Patients cannot restrict their own health information from being contributed to NEHR by HCSA licensees and approved contributors. For patient safety reasons, the Bill will require key health information of all individuals to be contributed to the NEHR. This is to minimise gaps in a patient's medical records.

- However, individuals may choose to restrict all healthcare providers from accessing their NEHR data. 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.

- Consequently, the individual may:

    - Experience more inefficient care delivery and may have to repeat laboratory or radiological investigations unnecessarily, and repeat critical information, such as allergic reactions to medications, at every consultation with a healthcare professional.

    - Similarly, caregivers will not be allowed to view the individual's HealthHub information via the caregivers' accounts if the individual has access restrictions in place.

    - Be unable to sign up for national healthcare initiatives that rely on sharing of health information, such as Healthier SG.

- The Bill will allow for such access restrictions to be overridden in the case of a medical emergency, also known as the Emergency Access Only or 'break glass' provision. For the 'break glass' override to be triggered, the individual must be:

    - Assessed by a doctor to be at risk of immediate and significant harm unless medical intervention is given, and

- Unable to provide consent (e.g., because they are comatose) or give consent for the doctor and supporting team to access their NEHR data for the purpose of the medical emergency. Individuals who retain mental capacity to provide consent also retain the right to refuse such access, even in a medical emergency.

- Further, individuals who have restricted access to their NEHR records should note that:

  - NEHR access restrictions may be overridden where required by other law or a court order.

  - Hospitals also access data through their internal electronic medical record systems, which are separate from the NEHR. Doctors will still access data outside of NEHR as part of their ethos and responsibility to provide the best possible care for the patient.

44. Why is patient data still being contributed after they have restricted access to their NEHR data?

- This is to prevent any gaps in the patient's records. Having a patient's records in the NEHR facilitates better and safer care provision across different healthcare settings and providers, especially if the patient chooses to allow full access to their NEHR again.

- This information may also be used in emergencies where patients are unconscious or are otherwise unable to provide the necessary information, and the information is required by providers to save the life of the patient. For more information on NEHR access in medical emergencies, please refer to FAQ 45.

45. What is the NEHR Emergency Access Only or "break glass" function? Can a patient refuse access to their own NEHR records in medical emergencies?

- When a patient's life is at risk, it may be necessary for the attending healthcare provider to have access to the patient's key medical records (e.g., information on allergies to medication).

- The Bill will allow for NEHR access restrictions to be overridden in the case of a medical emergency, also known as the Emergency Access Only or 'break glass' provision.

- For the 'break glass' override to be triggered, the individual must be:

    - Assessed by a doctor to be at risk of immediate and significant harm unless medical intervention is given, and the information in NEHR is necessary for the medical intervention, and

    - Unable to provide consent (e.g., because they are comatose).

- If the patient is capable of providing consent, the healthcare professional should ask the patient for consent to activate the Emergency Access Only function, and if the patient continues to refuse, the healthcare professional should respect the patient's wishes.

- To illustrate,

    - A patient who has just been involved in a road accident and is comatose may have his or her NEHR records accessed because the medical practitioner needs to check the patient's medication allergies to provide appropriate treatment. Such access will be enabled by the Bill.

    - Conversely, the medical practitioner cannot access the NEHR records if instead the patient has sustained severe injuries (e.g., broken limbs with major bleeding) but is not comatose and refuses to grant access despite being severely injured. The individual will be assumed to have considered the risk of not enabling access to his or her NEHR, including if the consequence may be life or death.

46. How does a patient restrict access to their NEHR data?

- At present, patients may restrict access to their NEHR by submitting a request at our public healthcare institutions (PHI). This would include obtaining and submitting the access restriction forms at one of the relevant departments in the PHI. More details can be found at Restricting Access to Your Health Information

or https://www.synapxe.sg/healthtech/national-programmes/national-electronic-health-record-nehr/faq.

- This will be further reviewed and details of the application process to restrict access will be made known prior to the mandatory contribution of key health information starting from end 2025.

47. Can MOH provide more patient access controls to give patients greater autonomy and control in who accesses their data?

- MOH recognises that patient privacy must be maintained. However, for the NEHR to fulfil its intended purpose of supporting continuity of care, healthcare providers need to have access to their patients' complete medical records.

- Introducing finer controls (e.g., allowing patients to restrict access to specific data fields or only allowing certain healthcare professionals to access their NEHR records) means that healthcare professionals cannot be sure that a patient's NEHR records are accurate or comprehensive, which would diminish the utility of NEHR in supporting healthcare professionals to provide patients with better and more seamless care.

48. Will patients be able to see their HealthHub records when they restrict access to NEHR?

- Individuals who have placed access restrictions on their own NEHR data are currently unable to view such information (such as vaccination records and laboratory tests) on their own HealthHub accounts, as this information is required to be drawn from the NEHR.

- However, MOH and Synapxe intends to enhance HealthHub to enable the viewing of such information for these individuals moving forward. This will allow individuals to monitor and track their own medical care and health plans. More details will be released in future, as some time will be required for HealthHub to make these changes.

- Sensitive Health Information (SHI) will continue to not be displayed in HealthHub to prevent inadvertent leakage. Individuals who require their SHI for any care

purposes can still obtain the required information directly from their respective healthcare institutions.

- Caregivers will not be allowed to view the HealthHub information of the individual under their care where that individual has placed access restrictions.

49. Can an individual restrict sharing of their data residing outside the NEHR?

- 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 under the HIB.

- Placing sharing restrictions means that data sharing by care providers for all use purposes enabled under the Bill will not be allowed for the said individual. The individual's consent must be sought, or the care provider must be able to justify data sharing through other legal means before sharing. MOH is developing a means for healthcare providers to check if the individual has restricted sharing.

- However,

    - To maintain seamless care for residents across the various public healthcare institutions and allow the Government to carry out national initiatives (like Healthier SG) and review its healthcare policies, individuals will not be able to restrict sharing of their data within the public healthcare ecosystem*.

    - The Ministry or its agent / representatives will still be allowed to initiate contact with you for enrolment in national healthcare programmes.

    - Data sharing outside of the purposes prescribed under the Bill – e.g., under other contractual means or other laws – may continue.

* The public healthcare ecosystem includes MOH, the Health Promotion Board, the Health Sciences Authority, the Ministry of Health (Holdings) Pte Ltd, the Ministry of

Health's Office for Healthcare Transformation, three public healthcare clusters (and their institutions), and the Agency for Integrated Care.

50. Why can public healthcare institutions still share data if a patient has restricted data sharing?

- Public healthcare institutions 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.

- MOH will ensure that there are safeguards protecting data shared and stored by the public healthcare sector.

51. What if I am willing to have my health information used for care purposes, but don't want to be contacted by MOH or its representatives for outreach purposes?

- Instead of placing legal restrictions on NEHR access and data sharing, individuals can decline to be contacted for outreach programmes, without affecting the collection and use of their health information for their care.

- For example, for Healthier SG outreach, individuals can choose to be placed on a Do-Not-Disturb (DND) list, like the Do-Not-Call registry which the Personal Data Protection Commission (PDPC) maintains. This allows individuals to continue enjoying the benefits of an up-to-date NEHR record, and data sharing under the Bill.

Section Nine: Cybersecurity and Data Security Safeguards

52. Who needs to comply with MOH's Cybersecurity and Data Security Safeguards?

- All HIB entities will have to meet a unified set of cybersecurity and data security requirements to protect both electronic and non-electronic health information.
- HIB entities include:
    - Healthcare providers contributing to or accessing NEHR,
    - Care providers participating in data sharing use cases enabled under the Bill.
- 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 surface area exposed to the threat of cyber-attacks and consequences of potential data losses.

53. What are some of the safeguards that MOH will be putting in place under the HIB to ensure entities put in place adequate cyber and data measures?

- MOH has developed a unified set of cyber and data security requirements ("**Cyber & Data Security Guidelines for Healthcare Providers**") in-consultation with CSA, IMDA and PDPC, that HIB entities need to comply with. The guidelines have been issued on 4 December 2023.
- The **Guidelines** allow entities an early opportunity to understand the requirements needed to improve their cyber and data security posture. This also provides them lead time to provide feedback as well as to comply with the future requirements.
- The latest Guidelines have been built on the MOH Healthcare Cybersecurity Essentials (HCSE) (issued on 6 Aug 2021) and data security requirements adapted from government data security standards, and have incorporated relevant requirements under CSA's Cyber Essential Mark and IMDA's Data

Protection Essentials respectively. For clarity, the Guidelines supersede the previously issued HCSE. More details on the Guidelines can be found here: MOH | Regulations, Guidelines and Circulars.

- Non-compliance to these requirements under the HIB may constitute an offence.

54. As HIB entities vary in their IT resourcing and capabilities as well as cyber/data readiness, what type of support will be available to HIB entities?

- MOH recognises that some healthcare providers may require additional support to adopt the requirements under the Guidelines and is currently developing an implementation support framework.
- We will be conducting a survey to better understand the current cyber and data security maturity levels of providers, including digitalization levels, to better assess the nature and type of support required.
- Notwithstanding, there are existing support schemes that HIB entities can consider tapping on:

Resource / Grant	Who is eligible?	What does this cover?	For more details
IMDA / ESG Productivity Solutions Grant (PSG)	Small-Medium Enterprises (SMEs)	- For pre-approved cybersecurity solutions including managed detection and response, unified threat management, and endpoint protection platforms. - 50% support for eligible companies, with an annual grant cap of S$30,000	https://www.enterprisesg.gov.sg/financial-support/productivity-solutions-grant https://www.gobusiness.gov.sg/productivity-solutions-grant/all-psg-solutions/
IMDA Chief Technology Officer-as-a-Service (CTO-aaS)	Small-Medium Enterprises (SMEs)	- CTO-aaS enables local SMEs to self-assess their digital readiness and needs, access market-proven and cost-effective digital solutions, and engage digital consultants for in-depth digital transformation strategy advisory and project management services under the SMEs Go Digital Programme.	https://www.imda.gov.sg/how-we-can-help/smes-go-digital/ctoaas https://www.imda.gov.sg/how-we-can-help/smes-go-digital

		- First-time usage of digital advisory and project management services is available at no cost to eligible enterprises. Subsequent usage or enhancement of services will be based on commercial agreements, should the enterprises want to continue to engage digital transformation consultants.	
CSA Cybersecurity Health Plan	Small-Medium Enterprises (SMEs)	- A scheme with funding support as well as Cybersecurity consultants (onboarded by CSA) who will take on the role of the SMEs' "Chief Information Security Officers" (CISO), akin to providing a CISO-as-a-Service (CISOaaS) to SMEs who may not have in-house cybersecurity personnel. The Cybersecurity Health Plan aims to tailor to SMEs' needs and prepare them to work towards attaining CSA's Cyber Essentials certification mark. - Up to 70% co-funding support upon signing up with the CISOaaS cybersecurity consultants onboarded by CSA.	https://www.csa.gov.sg/our-programmes/support-for-enterprises/sg-cyber-safe-programme/cybersecurity-certification-scheme-for-organisation/cybersecurity-health-plan
NCSS Tech-and-Go! Scheme	Social Service Agencies (SSAs)	- The National Council of Social Service (NCSS)'s Tech-and-GO! Scheme is a one-stop tech hub that supports Social Service Agencies (SSAs) in terms of grants, advisory, and consultancy services on how agencies can digitalise.	https://www.ncss.gov.sg/our-initiatives/tech-and-go/funding-support

55. How will the HIB interact with the PDPA?

- The HIB seeks to complement the PDPA by making clear what health information may be shared, by whom, and for what reasons. The HIB also prescribes sector-specific data security requirements in relation to the sharing of health information. Where there are differences in requirements between the HIB and

PDPA, the HIB requirements will supersede the PDPA requirements. For instance, the HIB data security requirements will supersede the PDPA as specific requirements on proper storage, reproduction, and transmission of health information to prevent unauthorised access is required, to better secure the sharing and use of health information.

56. What is the scope of the HIB security requirements?

- The HIB security requirements apply to healthcare providers with systems (e.g., desktops, laptops, servers, or devices) that either:

    1. contain health information or
    2. connect with other systems containing health information.

- Standalone systems (i.e., not connected with other systems containing health information) that purely store non-health information (e.g., financial data) are excluded from the scope of the HIB security requirements. Nonetheless, the cybersecurity requirements set out in the Guidelines are also relevant for such systems as part of holistic cyber defence. For avoidance of doubt, applicable data security requirements will still apply to healthcare providers on pen-and-paper records.

- While the HIB security requirements do not prescribe detailed requirements on healthcare providers' third-party vendors, products, or services (e.g., Clinical Management Systems (CMSes), cloud storage services), healthcare providers shall ensure that their choice of third-party vendors, products, or services is able to support them in meeting the HIB security requirements. Nonetheless, data intermediaries such as CMSes will be required to meet broad obligations under the HIB.

57. Do I need to implement all the security requirements? What if I'm unable to meet some of them?

- All healthcare providers will need to meet the same endpoint HIB security requirements – selectively applying a subset of the cyber/data requirements would compromise the HIB entity's endpoint systems and devices, and data security of health information. For instance, measures such as the proper

tracking of hardware and software asset inventory, governing the access rights to certain hardware and software, and installing anti-malware solutions on assets should be implemented collectively to properly safeguard the confidentiality, integrity and availability of systems and data.

- The security requirements are intended as a baseline set of cyber and data hygiene requirements to secure the IT assets of a small healthcare provider (e.g., standalone GP clinics).

- MOH will be conducting a survey to study the current cyber/data readiness and digitalisation levels of HIB entities. The findings will allow us to determine if and how much implementation support would be required to help uplift entities' cyber and data security posture.

58. Are there any additional security requirements if I need to access and / or contribute data to the NEHR?

- The HIB security requirements are intended as minimum standards for all HIB entities, regardless of whether they need to access and / or contribute data to the NEHR.

- Depending on whether there is a need to connect to and contribute data to the NEHR, HIB entities will in turn need to meet the necessary security / connectivity requirements, as part of NEHR onboarding, before your systems are allowed to connect to the NEHR.

59. Do we have to implement all the security requirements if our health records are maintained as paper records, and we do not have system integration or interface with NEHR?

- Cybersecurity requirements might not be applicable in this instance if you are still on pen-and-paper, though the applicable data security requirements would still be relevant.

- However, if you, for instance, provide an Active Ageing Centre (AAC) service which may need to share or receive non-NEHR data under HIB, and this is done by way of a system, the cybersecurity requirements may also be applicable.

60. When will the security requirements be implemented or enforced?

- While the requirements have been issued as guidelines since 4 December 2023, to promote early awareness and familiarity amongst the HIB entities, they would be enforced as regulatory requirements under the HIB when directed by the MOH at a later timepoint.

- The requirements are expected to be implemented in phases, taking into account the following:

    - sectoral readiness and prevailing capabilities;
    - availability of implementation support plans to uplift cyber and data security posture; and
    - when mandatory data contribution to the NEHR will be enforced.

61. Will healthcare providers be audited to assess the level of compliance with the security requirements?

- When the security requirements are eventually imposed as regulatory requirements, selective audits may be conducted to check compliance.

- Healthcare providers will also be required to self-declare their compliance with the requirements. MOH strongly encourages providers to conduct periodic internal checks and assessments, to establish their own cyber and data security readiness, and make effort to improve their security posture and comply with the future HIB requirements.

62. I run a small private practice / day care service. Is there really a need for me to establish security policies and processes for my practice? Isn't this too onerous?

- While we recognise that it may be challenging for smaller healthcare providers (e.g., solo practitioners, small community care service providers) to establish and document security policies for your practice, such services collect and store important patient information (e.g., patient identifiers, medical conditions) which warrants appropriate safeguards to ensure the security, confidentiality, integrity, and availability of patient data.

- The intent is to encourage healthcare providers to consider key security practices that should be in place as part of your clinical operation to ensure the security, confidentiality, integrity and availability of your IT assets, systems, and patient data. That said, you are encouraged to translate the Guidelines into policies and processes appropriate for your practice.

63. What are the expected costs of compliance with MOH's cybersecurity and data security requirements? How is MOH supporting healthcare providers to meet these requirements?

- While there will be some added costs, such as in terms of skilled manpower, procurement of cybersecurity solutions, and upskilling in cyber/data security competencies, MOH is studying the necessity of providing added implementation support for healthcare providers, especially smaller ones such as our SMEs, to meet the requirements.

- In the meantime, there are some available schemes such as the IMDA / ESG Productivity Solutions Grant (PSG) and IMDA Chief Technology Officer-as-a-Service which offers a co-funding element. In the longer run, healthcare providers should consider cyber and data security as a critical component of their clinical operations, and which should be factored in their operating cost.

64. Will IT vendors be held accountable if cybersecurity breaches are due to insufficient security standards on their part?

- Yes, the HIB is intended to allow MOH to take IT vendors to task depending on the facts of the case. This ensures appropriate right-siting of accountabilities. For instance, where investigations reveal that the IT vendor / data intermediary had insufficient security safeguards resulting in a severe health data breach, MOH would be empowered to investigate the organisation and mete out penalties under the HIB. MOH is reviewing the specific obligations and security requirements that indirect third-party providers (e.g., clinical management system vendors) will be required to meet under HIB.

- That said, the onus is also on healthcare providers to ensure their IT vendors have appropriate security standards in place.

65. Under what circumstances should cyber / data incidents be reported to MOH? What are the reporting requirements and timelines to comply with?

- The HIB would be prescribing the scope of the notifiable cyber or data incidents:

Proposed Incident Reporting Thresholds & Timelines under the HIB

	Cybersecurity Incidents	Data Breaches
Reporting Thresholds	• A notifiable^ cybersecurity incident involves: i. a computer or computer system containing health information or interconnected with a computer or computer system containing health information; and ii. The computer or computer systems are under the healthcare provider's control.	• Aligned to PDPA's data breach notification threshold. • In the context of health information, a notifiable data breach is one that: i. results in, or is likely to result in, significant harm to an affected individual (i.e., breach contains sensitive health information); or ii. is, or is likely to be, of a significant scale (i.e., impact on equal or more than 500 affected individuals).
Reporting Requirements	• Initial notification to MOH within 2 hours after healthcare provider assesses that the incident is a notifiable cybersecurity incident or data breach meeting the reporting thresholds. • Affected healthcare provider to provide an incident report within 14 days of initial notification. • Healthcare provider must notify affected individuals at the same time, or as soon as practicable after notifying MOH, if the incident causes, or is likely to cause significant harm to an individual.	

- The following are examples of what need not be reported to MOH under the Bill:

  - IT system or infrastructural failure not caused by a cyber-attack. For example, power failures due to severe weather events.

  - Data breaches involving only non-health information (e.g., financial data, account login details non-attributable to the provision of a healthcare service). Nonetheless, such data breaches should still be reported to PDPC if it meets the PDPA's data breach notification criteria.

^Notifiable cybersecurity incidents include but are not limited to e.g., unauthorised hacking of computer or computer systems, installation or execution of unauthorised software or computer codes of malicious nature, attempts to prevent the availability of computer information or services to its intended users (i.e., denial of service attacks), attempts to intercept the traffic between two computer or computer systems to steal or alter information (i.e., man-in-the-middle attack), etc.

Section Ten: Requirements for Data Intermediaries

66. What are Data Intermediaries?

- 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 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. Organisations that process health information on behalf of a healthcare provider, but for purposes not prescribed under the Bill, are out of scope.
- For example, an organisation helping a clinic collect and process health information from patients specifically for the clinic's own purposes (e.g., third-party administrators for billing matters, research firms for patient surveys) are not data intermediaries under the Bill. However, PDPA's obligations for data intermediaries will still apply to these organisations.

67. What are Data Intermediaries' obligations under the HIB?

- The Bill will impose several obligations on data intermediaries, including:
    - Protecting health information from unauthorised access or disclosure,
    - Disposing of information that is no longer needed,
    - Ensuring data portability standards, and
    - Informing the entity of any cybersecurity incident or data breach without undue delay.
- This is similar with PDPA's approach, and consistent with international standards (such as USA's Health Insurance Portability and Accountability Act) that delineate accountability between the data controller and data processer.
- 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.

68. What are a HIB entity's responsibilities with respect to Data Intermediaries?

- HIB entities should use only data intermediaries which provide sufficient safeguards so that their processing of health information will 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.

Section Eleven: Enforcement and Penalties

69. How will MOH enforce the HIB?

- In general, MOH will conduct sample audits to ensure compliance with specific requirements, such as the entities' cybersecurity and data security standards.
- Members of public can report any access, collection, use, disclosure and retention of health information that do not comply with the requirements stipulated in the Bill. These may include:
    - Unauthorised access to a patient's NEHR records, as detected from the individual's NEHR access history on HealthHub.
    - Unauthorised disclosure and sharing of a patient's health information when the patient has restricted sharing of health information residing outside of NEHR.

70. What are the general powers MOH intends to have under the HIB?

- To ensure that all the requirements under the Bill are complied with and non-compliances dealt with in a timely and appropriate manner, MOH intends to have powers under the Bill to issue directions for entities to rectify non-compliances with the Bill.
- Such powers include directing entities to:
    - Stop unauthorised access to health information on the NEHR,
    - Destroy all health information collected in an unauthorised manner,
    - Stop further unauthorised sharing of health information under the data sharing framework,
    - Comply with cyber and data security requirements.
- The Bill will also provide powers to investigate any non-compliances with the Bill, such as the powers to obtain information, and powers of inspection, entry, and search.

71. What is the intended penalty framework under the HIB?

- 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.

- For severe non-compliances by entities, MOH proposes to impose a fine of up to S$1 million, or 10% of the organization's annual turnover (whichever is higher). An example of such non-compliance is a data breach that results in the disclosure of patients' sensitive health information. This approach is aligned with the PDPA's penalty regime for non-compliances.

- 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.

72. What are the penalties for individuals under the HIB?

- Beyond organisational accountability, MOH will strengthen the accountability of individuals who handle or have access to health information.

- MOH will introduce the following offences under the Bill to hold individuals accountable for egregious mishandling of health information in the possession of or under the control of a HIB entity:

    - Unauthorised disclosure, or conduct causing the disclosure of health information.

    - Unauthorised use of health information to obtain a gain, or cause harm or loss to another person;

    - Re-identification of anonymised health information.

- The individual-level offences under the Bill will supersede S48D, S48E and S48F of the PDPA, which cover offences regarding the egregious mishandling of personal data by individuals.

- Despite introducing these individual offences, MOH considers that organisations are primarily accountable for the security of health information. Employees acting in accordance with their employer's policies and practices, or whose actions are authorised by their employers, will not run the risk of such penalties.