Contents

Annex A: Key Concepts and Proposed Provisions of the Health Information Bill

This Annex covers the key concepts and seeks to explain the proposed provisions within the Health Information Bill. The annex is divided into 7 sections:

I.What is Health Information

Health information is data relating to one's medical history, which helps healthcare providers offer and deliver informed care to the patient. Health information includes both an individual's administrative data and clinical data.

Administrative data 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 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 befrienders.

Clinical data refers to all information related to (i) the physical and mental health of the patient, and (ii) diagnoses, 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.

II.Key Provisions and Administration of the Health Information Bill

1. The Bill will govern the collection, access, use, and sharing of selected health information in a safe and secure manner across various healthcare settings, so as to enable better continuity and transition of care and support outreach efforts. The key provisions of the Bill are as follow:

(a) Providers licensed under the Healthcare Services Act ("HCSA Licensees") will be mandated to contribute selected health information to the NEHR. Approved contributors such as retail pharmacists will also be mandated to contribute relevant information where generated.

- There are many benefits that the NEHR can provide for healthcare. The availability of health information in the NEHR reduces the need for duplicate tests or history taking. Currently, only public healthcare institutions and some GPs contribute this information, which limits the usefulness of NEHR as a comprehensive record of key aspects of a patient's medical history. Mandating all healthcare licensees to contribute information to the NEHR expands the scope of the NEHR significantly, and will help reduce the gaps in patients' medical histories.
- Approved contributors are organisations which are envisioned to generate data which is useful to be stored in the NEHR. As such, they will be mandated to contribute relevant information to the NEHR as well.

(b) Only healthcare licensees and approved users will be allowed to access health information in the NEHR for patient care purposes.

- The NEHR may only be accessed by either licensees or approved users for direct patient care purposes, or where such use is required for under other written laws (e.g., for criminal investigation, assessment to bear firearms). The information held within the NEHR is sensitive and unauthorised access and use will be met with strict penalties.

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

- There exists a wealth of information beyond the NEHR, and these may be more accurate or detailed than what the NEHR holds. There are many different data sharing frameworks in place today. These can be contractual or legislative. This results in the data sharing landscape being fragmented, and unnecessarily complex. Providers are hesitant to share patient information with other providers for fear of infringing patient confidentiality, particularly where the sharing is done without first obtaining patient consent. The Bill will simplify the health data sharing framework and provide greater clarity on the boundaries of data sharing. This will help facilitate the flow of information between providers for patient care purposes.

- Social services are also playing an increasingly important part in the delivery of healthcare (e.g., Active Ageing Centres). As such, beyond healthcare providers, the Bill will introduce and enable sharing of health information to selected social care services.

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

- With increased data sharing among healthcare providers, the surface area for cyber-attacks and data breaches will increase. The expanded use of digital technologies and devices in the healthcare sector also creates the potential for new cybersecurity vulnerabilities to appear. It is therefore important to implement clear and stringent safeguards against such risks, and for users to take greater responsibility for data access.
- At the same time, such safeguards come with both operational and legal burdens on providers. The Bill aims to find an appropriate balance, and provide clarity on the roles and responsibilities of entities that fall within scope. Under the Bill, entities, healthcare professionals or third-party IT vendors can be held liable for cyber and data security breaches, depending on the facts of the case.

Administration of the Bill

2. The Bill will be administered by the Minister for Health ("the Minister"). The Minister will be empowered to appoint any of the following individuals to exercise any or all of the powers conferred or duties imposed on the Minister under the Bill (except for the powers of appointment and delegation):

(a) a public officer, an officer of any public authority, or any other individual who is suitably qualified, to be an authorised officer for the purposes of that provision, either generally or in a particular case;

(b) a public officer to be an investigation officer.

III. Provisions relating to the National Electronic Health Record

Provisions on Contribution to NEHR

3. The NEHR is a secure centralised repository of heath information established in 2011 and is intended to serve as a source of information for users of the system. The NEHR has been progressively deployed to both public and private healthcare institutions across Singapore to support the aim of "One Patient, One Health Record". Currently, only public healthcare institutions and some private GPs contribute information to the NEHR.

4. **The Bill will mandate all healthcare licensees to contribute a copy of selected key health information to the NEHR. MOH will be empowered to approve other healthcare providers ("approved contributors") to contribute to the NEHR. Such approval will include the types of health information that approved contributors must contribute to the NEHR.**

5. Not all health information will be contributed to the NEHR. Only information that is expected to be generally beneficial to all providers will be mandated for contribution. This includes:

(a) Patient Demographics (e.g., name, address, contact details)
(b) Visits (e.g., admission to a hospital, GP visit)
(c) Medical Diagnosis / Allergies
(d) Operating Theatre Notes / Procedures / Treatments (e.g., endoscopy, surgical reports)
(e) Discharge Summaries
(f) Medications
(g) Investigation Reports (e.g., laboratory reports such as blood tests, radiological investigation reports such as X-Ray Reports)

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

6. 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 as such granularity may not be beneficial or applicable through the various settings. It would also make the system unwieldy to navigate.

7. **The Bill will differentiate the types of data that the respective classes of healthcare providers will need to contribute based on the role that organisation plays in a patient's healthcare journey. Notwithstanding this, the Bill will only require healthcare providers to contribute the information where 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 particular visit. The GP would also not be required to contribute laboratory test results, as such tests are not conducted by the GP himself, but by a clinical laboratory. The clinical laboratory will then need to contribute information on the test results to the NEHR.

8. The Bill will also not require healthcare providers to contribute data of every individual to the NEHR as there is minimal benefit in doing so for certain groups of individuals. For instance, the data of short-term visit pass holders (STVP) will not be required to be contributed to the NEHR. STVP holders are unlikely to remain in the healthcare system long enough to meaningfully benefit from the NEHR, and the costs of storing their information would outweigh the potential health benefits they may receive. For example, there is no need to store the records of tourists who may fall ill while on a holiday and visit a doctor in Singapore.

9. Please refer to **Annex B** for the specific data fields that need to be contributed for the various users of NEHR.

Provisions on Access to NEHR

10. **The Bill will allow healthcare licensees and approved users access to the NEHR. Both healthcare licensees and approved users will require MOH authorisation for this access. Licensees will be authorised via a licence issued to them under the Healthcare Services Act (HCSA). Other non-HCSA licensees who require access to the NEHR will be required to submit their application to MOH for review and be granted access before they can access the NEHR.**

11. Licensees and users who have been granted access rights can view the health information of an individual only for the purposes prescribed in the Bill or for purposes which Minister may authorise. Such access is only currently allowed for direct patient care and where statutorily required by other written laws.

12. "Patient care" in relation to the Bill means the provision of a healthcare service to the individual. Beyond clinical matters, "patient care" includes any administrative matter directly related to the provision of the healthcare service to the individual, such as the following:

(a) the individual's admission to, and discharge from, the care of a person providing the healthcare service to the individual;
(b) the scheduling of the individual's appointments with the person providing the healthcare service to the individual; and
(c) the transfer or referral of the individual by the person providing the healthcare service to another person who provides or may provide any healthcare service to the individual.

13. Licensees and users may also access the NEHR of individuals **where required by certain other laws**, usually as part of a statutory medical examination (see **Table A** below). The Bill will prescribe these allowable use cases, which include for example, the assessment of an individual's fitness to bear firearms (such as in the Enlistment Act). 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 provide their consent.

Table A: 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)

14. Unless the individual is a patient who has established a care relationship with the care provider, users are not allowed to access the NEHR records of the individual, even with the individual's consent. To illustrate using two scenarios:

(a) An individual cannot ask for their NEHR records to be accessed by a family member who may be a medical practitioner, but not registered under their care.
(b) A medical practitioner may not access the records of a patient upon referral, where the patient has not made an appointment or has not made known to the medical practitioner that they intend to receive care from the medical practitioner. Only after an appointment with a care provider is made can the medical practitioner access the NEHR records, as this qualifies that a care relationship has been established.

15. The Bill prohibits the direct access of the NEHR for the purposes of:

(a) determining an individual's suitability or eligibility for employment, including
    i. promotion in employment or office,
    ii. continuance in employment or office, or
    iii. removal from employment or office; and

(b) insurance or insurance-related matters, including
    i. deciding whether to insure any individual or to continue or renew the insurance,
    ii. making a claim on the insurance of any individual, or
    iii. processing a claim made on the insurance of any individual.

16. As the purposes for which NEHR can be accessed is envisioned to change over time, the Bill also enables MOH to introduce new prohibitions or allowable access purposes from time to time.

17. The Bill will empower any individual to request for access restrictions to be placed on their health information which resides in the NEHR, i.e., to block all providers from accessing their data. However, to ensure that patients' NEHR health information remains up-to-date, especially if they remove the access restriction again, mandated

information will still be contributed on the back end to the NEHR. The section on Access and Sharing Restrictions covers this in more detail.

Further Safeguards on NEHR Contribution and Access

18. Beyond the legal provisions under the proposed Bill, MOH will also put in place other administrative requirements to safeguard health information and to provide guidance to medical professionals on how to use the NEHR. MOH will also issue guidelines which aim to outline the core ethical principles and reasonable professional standards that should be adopted when contributing to, accessing, or using NEHR. You may wish to refer to the Guidelines on Appropriate Use and Access to National Electronic Health Records[1].

Sensitive Health Information

19. While all health information will be protected by the security requirements placed on the NEHR, further measures will be imposed when users attempt to access certain types of information which are deemed to be more sensitive ("Sensitive Health Information" or "SHI"). The full list of SHI that warrants additional protection in NEHR is aligned with the whitelist of specified medical information under the Personal Data Protection (Notification of Data Breaches) Regulations. Some examples include health information in relation to a termination of pregnancy or sexually transmitted diseases.

20. MOH has administratively placed additional access controls as we are aware that knowledge of such items may predispose an individual to discrimination or increase their risk of being stigmatised by society at large. This information resides behind a double log-in mechanism, and requires users to make a conscious decision to access such information. Access to SHI is determined by the user's role in the care for the patients, and relevance to their practice. Not all healthcare professionals would require information on SHIs to carry out their duties. For example, medical practitioners would have access to sensitive health information as it is relevant for them to know this when treating their patients, but physiotherapists currently may not.

21. While the patient's consent is not generally required to access SHI as they are deemed to have granted consent at the point of seeking care, the professional may still choose to do so. Nonetheless, granting such 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. Access to SHI will be audited. Inappropriate access to SHI or subsequent disclosure may constitute an offence under the Bill or other written laws (e.g., the Infectious Diseases Act). Users who are found guilty will be penalised accordingly. Entities will also be mandated to report data breaches involving the SHI of one or more individuals to MOH, and to notify the affected individuals within stipulated timeframes under the Bill (you may refer to **Mandatory Incident Notification Requirement** for more details).

[1] The Guidelines may be found on the same website as this document.

Guidelines on Appropriate Use and Access of the NEHR

22. To guide clinicians on the appropriate usage of NEHR, MOH will also issue guidelines which aim to outline the core ethical principles and reasonable professional standards that should be adopted when contributing to, accessing, or using NEHR. You may wish to refer to the Guidelines on Appropriate Use and Access to NEHR[2]. 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.

[2] The Guidelines can be downloaded on the same website as this document.

IV. Provisions relating to non-NEHR Data Sharing for Specified Purposes

23. The second key aspect of the Bill is to enable **non-NEHR** data sharing for prescribed purposes. This refers to sharing of data that resides outside the NEHR (e.g., the hospital's electronic medical records, clinical notes of the GP). As the number of care providers in the community healthcare and social care field continues to grow, there is a greater demand for health information to be shared to ensure better care quality.

24. **The Bill also formalises data sharing arrangements, to allow specific types of data to be shared with specific parties for specific care purposes, and will take precedence over Personal Data Protection Act (PDPA) requirements. This data sharing can happen between both Public Healthcare Institutions as well as private sector healthcare providers, and healthcare providers will be specifically appointed under the Bill to receive and share data.**

25. Data sharing provides wide ranging benefits, such as a more seamless experience of the healthcare system and care transition. It also enables MOH and our partners to administer certain initiatives, such as financial assistance schemes. However, we recognise that there is a need to balance between the benefits of data sharing and the potential risks of exposure should there be unauthorised or illegitimate use of the data.

Provisions on purposes for which non-NEHR data can be shared

26. Data sharing will be scoped to what is necessary for the allowable use 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 variables must be fulfilled for the data sharing to take place. Should any one variable not be met for the use purpose, the healthcare provider is unable to use the Bill as the legal basis for such sharing. In such circumstances, the healthcare provider should explore if they are able to share the data if such data sharing is permissible under other written laws.

27. There will be three allowable use purposes prescribed under the Bill:

(a) outreach under national healthcare initiatives;
(b) supporting continuity of care including telecollaboration; and
(c) eligibility assessment for financing schemes.

Table B below sets out the use purposes, care providers, and types of data that can be shared under the Bill.

28. Data may be shared in two directions – either downstream to the receiving care provider, or upstream (shared back to the provider which originally disclosed the data). In some cases, data is only envisioned to be shared downstream, as thereafter patient consent may be sought before any further data sharing takes place.

Table B: Proposed use purposes, care providers and types of data that can be shared under the Bill				
Sharing Healthcare provider	Direction	Receiving Healthcare provider	Data Categories	Use purposes
MOH entity	Share with or receive from	• MOH entity	Administrative and/or clinical data	Any of the 3 use purposes defined in Para 25
MOH entity	Share with	• Primary Care Network Headquarters (PCN HQ) • General Practitioners • Sport Singapore • Active Ageing Centres • Community Health Centres • Social Service Organisations / Agencies[1]		
Public healthcare clusters and their institutions Agency for integrated care (AIC)	Share with or receive from	• Public Service Agencies		
PCN HQ and GPs	Share with	• PCN HQ / GPs • Active Ageing Centres • Social Service Organisations / Agencies • AIC		

<u>How to read the table:</u>
The table should be read from left to right.

For example – under the first row, a MOH entity (X) may share with another MOH entity (Y), any administrative or clinical data for any of the three listed use purposes. As the data sharing can be done upstream, this means entity Y may also share with entity X, any administrative or clinical data for any of the three listed use purposes.

[1] Social Service Organisations and Agencies refer to organisations which provide healthcare, social care services, or a mix of both, and include services run by voluntary welfare organisations (VWOs). Some examples include VWO-run nursing homes, palliative care services, home medical services.

29. To illustrate, an active ageing centre (AAC) intending to share data with another AAC for outreach purposes will **not** be able to do so as AACs are not enabled to share data under the Bill. If the AAC wishes to continue sharing, they may need to find other legal or contractual basis to do so, such as obtaining proper informed consent from the individual.

Provisions on conditions for non-NEHR data sharing

30. **The Bill will set out the purposes for which health information residing outside the NEHR can be shared, and, specific to each purpose: (i) the types of health information that may be shared, (ii) the care providers which may share such information, and (iii) the care providers which may receive such information**.

31. While the NEHR is a crucial source of health information, it only contains a subset of all health information generated in the ecosystem. The bulk of health information continues to reside within each healthcare provider's health record systems, such as the electronic medical records (EMR) of a hospital or the clinic management system (CMS) of an outpatient clinic. Such information remains equally, if not more, important for the provision of informed care to the patient. Thus, it is important that health information outside of the NEHR be enabled to flow between relevant health providers for certain specified purposes.

(a) 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.

32. If care providers wish to share health information for purposes not provided in the Bill, they will not be able to rely on the Bill for such sharing. They will need to find a legal basis, for example, to obtain patients' explicit consent, or where provided for under other written laws.

33. Even if the purpose, provider, and dataset have been specified in the Bill, it does not automatically grant care providers the right to share data carte blanche. Care providers (both sharing and receiving) must meet the requirements stipulated within the Bill (for example, having the receiving entity's acknowledgement that it has met the appropriate cyber and data security requirements) before they engage in data sharing.

34. The Bill will require both disclosing and receiving healthcare providers to comply with the following conditions for sharing, prior to any data sharing taking place.

(a) Both the disclosing healthcare provider and the receiving healthcare provider must:

i. Agree to share and receive the data, respectively. The Bill will require that a request be put up by the receiving healthcare provider to the disclosing healthcare provider to share the required data. This ensures that both parties are aware that data will be shared, and can take the necessary steps to ensure that they comply with the requirements to share such data.
ii. Appoint, and make known to each other, the persons who can disclose or receive such data, respectively.
iii. Agree upon the time period and frequency of sharing.

(b) Disclosing healthcare providers must:
i. Not share data of individuals who have placed access restrictions on their NEHR records or sharing restrictions for data residing outside the NEHR. MOH is developing a means for healthcare providers to check if the individual has placed such access or sharing restrictions;
ii. Have taken reasonable steps to ensure that the information being disclosed is accurate, up to date, complete, relevant, and not misleading at the point of creation.
iii. Make reasonable efforts to limit the disclosure of the health information, to the receiving party, to the minimum necessary to facilitate the request.
iv. Ensure that receiving healthcare providers must have met the relevant cybersecurity and data security requirements.

(c) Receiving healthcare providers must:
i. Not share the disclosed data with any other healthcare providers, unless this is specifically allowed for by the disclosing party.
ii. Not use any data disclosed to them for purposes such as data analysis, research, or quality improvement; or refining, changing or developing the way a healthcare service or a community healthcare service is provided to any individual.

35. The Bill will prohibit the disclosure of individually-identifiable health information of a deceased individual, unless the disclosure is in relation to the cause of death. This allows for healthcare providers to inform each other about a patient's death.

36. 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.

Sharing of anonymised or aggregate level information by MOH

37. The Bill will allow the Minister to approve the disclosure of non-individually identifiable health information from MOH to a Government department or public authority or any other person, subject to any condition that the Minister thinks fit.

(a) Health information can benefit research and government policy review, to improve issues such as population health or develop medical treatments.

(b) Safeguards will be put in place to prevent unauthorised use by the entities who have received the data. These include prohibiting the care provider from re-identifying any individual from the dataset or sharing the data onwards to other parties, or face stiff penalties.

V.Access and Sharing Restrictions

38. **The Bill will provide individuals the option to place access restrictions on 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. The restriction will also apply to any statutory medical examination that the individual may be required to undergo. 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 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.

39. **The customisation of access restriction to specific requests (e.g., to restrict access only to specific doctors, institutions, or certain data fields) will not be allowed, to safeguard patients' safety and wellbeing**. Missing records can increase health risks and potential for harm to the patient. For example, patients may not wish to share that they were an organ recipient. However, such information is key to medical practitioners as it informs them that the patient may be immunocompromised, and certain treatments may be contraindicated. Blocking information might also cause medical practitioners to miss out on pertinent information in formulating their treatment plan for their patient, for e.g., serious drug-drug interactions. If medical practitioners do not know whether the information they see in the NEHR is a complete record, its utility will be severely diminished.

Situations in which NEHR access restrictions can be overridden

40. The Bill will allow healthcare professionals to override NEHR access restrictions in two scenarios:

(a) medical emergencies, or
(b) where required by prescribed laws.

41. In medical emergencies, a healthcare professional can decide to override the access restrictions only if all the following criteria is fulfilled:

(a) The patient's life is deemed to be at risk, and the patient is at risk of gross disability, pain, or distress, unless there is immediate medical intervention, and such intervention is in the patient's best interest; and
(b) The patient is unable to provide consent.

42. To avoid doubt, professionals are not allowed to access the NEHR records of patients who have placed access restrictions on their NEHR records and have the capacity to provide consent even while in the medical emergency, but still refuse to allow access.

(a) 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 his or her 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 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.

43. Before using the Emergency Access Only function, the healthcare professional must declare and document that (a) they are accessing NEHR for a medical emergency, (b) access to the NEHR is required to assist with the medical intervention, and (c) provide a reason for the access.

44. Healthcare professionals who misuse the Emergency Access Only function may be subject to legal penalties under the Bill and disciplinary action from the relevant professional bodies, such as the Singapore Medical Council.

45. For completeness, where access restrictions have been placed

(a) All individuals will continue to be able to view information drawn from the NEHR (such as vaccination records and laboratory tests) on their own HealthHub accounts, to allow them to monitor and track their own medical care and health plans. For minors (aged below 21), the same applies and parents will continue to be able to view their minor child's HealthHub information. We will continue **not** to display SHI in HealthHub to maintain the security of these sensitive information and prevent against inadvertent leakage. Individuals who require 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.

(b) Caregivers will not be allowed to view the HealthHub information of the individual under their care where he or she has placed access restrictions.

Implications of Access Restrictions on other (non-NEHR) data sharing

46. An individual who has placed access restrictions on their NEHR data will also be deemed to have restricted sharing of their health information residing outside the NEHR, and vice versa. Individuals will not be able to restrict only one without the other.

47. Placing sharing restrictions mean 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, for example, patients' explicit consent, or other written laws, before they can engage in such sharing. MOH is developing a means for

healthcare providers to check if the individual has placed such access or sharing restrictions.

48. Individuals will not be able to restrict sharing of their health information within the public healthcare ecosystem. This 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. Sharing within the public healthcare ecosystem is essential to maintain seamless care for Singapore residents should they seek care at any public healthcare institution, as well as for the Government to carry out national initiatives (like Healthier SG), and review its healthcare policies. To avoid any doubt, this only refers to health information residing outside the NEHR (i.e., in the institutions electronic medical records). Any access restriction put in place by the individual will continue to apply.

49. Alternatively, 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, similar to 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.

VI. Provisions relating to Cybersecurity and Data Security

50. As custodians of patients' healthcare information, entities that contribute data to and/or access the NEHR, or engage in data sharing enabled under the Bill, are required to meet a unified set of cybersecurity and data security requirements ("cyber/data requirements"). These 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. The Cyber and Data Security Guidelines for Healthcare Providers, released on 4 December 2023, provide guidance on the cyber and data security measures to be put in place to safeguard their patients' health data, in the lead up to the implementation of the HIB.

51. Even if an organisation is a prescribed entity under the Bill, the cyber/data requirements will not apply to the entity if it neither contributes to / access the NEHR, nor engages in a prescribed data sharing use case enabled under the Bill. Nonetheless, as a matter of good practice, healthcare and community care providers should strongly consider adopting the security requirements since the healthcare system is increasingly digitalised and interconnected, and security threats are on the rise.

52. Public sector agencies that are prescribed entities under the Bill are not legally required to meet the cybersecurity and data security requirements under the Bill, as they and their employees already need to comply with requirements under the Government Instruction Manual for ICT&SS Management (IM8).

Cybersecurity and Data Security Requirements

53. The following cybersecurity requirements apply to entities' computers and systems that either i) contain health information, or ii) communicate with other systems containing health information. While these requirements, as indicated in MOH's Cyber and Data Security Guidelines for Healthcare Providers, are more prescriptive, what will eventually be prescribed in the HIB and its corresponding subsidiary legislation will be pitched at a broader level. See **Annex C** for more details of the requirements.

Cybersecurity
Updates – *software updates* • Install software updates on your devices and systems promptly.
Secure/Protect – *virus/malware protection, access control, secure configuration* • Use anti-malware and anti-virus solutions to protect against malicious software. • Implement access control measures to control access to your data and services. • Use secure settings for your organisation's procured hardware & software.

Backup – *back up essential data* • Back up essential data and store them offline.
Asset – *people, hardware & software, data* • Equip staff with cyber-hygiene practices as the first line of defence. • Identify the hardware and software used in your organisation, and protect them. • Identify the type of data your organisation has, where they are stored, and secure them.

54. The data security requirements apply to all electronic and non-electronic health information possessed by, or under the control of the entities. See **Annex C** for more details of the requirements.

Data Security
Secure – *storage, reproduction, and conveyance requirements* • Store your health information securely to prevent unauthorised access. • Do not reproduce copies of sensitive health information unless necessary. • Transport health information properly to avoid unwanted data exposure
Identify – *data security classification, marking requirements* • Know the information sensitivity levels of the data to apply appropriate safeguards. • Differentiate data of varying information sensitivity levels by marking their classification.
Access – *authorised users* • Restrict access to health information for valid and relevant purposes.

55. HIB healthcare providers must also comply with the following general requirements. See **Annex C** for more details of the requirements.

Common Cyber & Data Requirements
Outsourcing & Vendor Management • Understand the responsibilities set between your organisation and vendor.
Incident Response • Prepared to detect, respond, and recover from incidents.

Disposal Requirements • Proper disposal of health information mitigates the risk of unauthorised access.
Emergency Planning for Contingency • Supports ability to withstand service disruptions to ensure business continuity.
Review Security & Internal Audit Requirements • Regular checks on corporate policies and processes to ensure compliance and identify vulnerabilities.

Provisions on Accountability and Compliance

56. The implementation of HIB's cybersecurity and data security requirements will be aligned to the implementation of the mandatory NEHR contribution, which is expected to start from end-2025.

57. There will be no approval or licensing regime for the entities in meeting the cyber and data security requirements. Instead, all entities will be required to self-declare their compliance with the requirements. This will provide assurance to patients that the entities have taken the necessary steps to implement the security requirements under the Bill, before they share data with, or receive data from other healthcare providers. Entities will also have the option to declare that they are unable to comply with the cybersecurity and data security requirements. They will then have to indicate the reasons for their inability to comply, and develop a plan to remediate the gaps, including a reasonable timeline of when they can eventually comply with the requirements. The failure to declare, or deliberate false declarations, will be an offence.

58. Entities will also be subject to cybersecurity and data security audits conducted randomly by MOH, and/or its appointed auditors.

59. Entities must designate one or more individuals, either within the entity or contracted externally, to be responsible for ensuring that the entity compiles with the requirements in the Bill, and for MOH to contact in the event of any data breach or cybersecurity incidents. This is similar to the requirements stipulated in Section 11-3 of the PDPA.

Mandatory Incident Notification Requirement

60. Prescribed entities under the Bill will be mandated to report any cybersecurity incidents or data breaches (collectively known as "incidents"). This is to ensure that entities are accountable for the health information in their care, and build confidence in the flow of data in the healthcare system. It will also enable entities to take timely actions to respond to and remediate potential incidents.

61. Under the Bill, MOH will be enabled to take the following steps in response to an incident notification:

(a) Coordinate and respond to incidents that may severely affect patient safety and privacy;
(b) Take mediation measures regarding the affected healthcare provider's involvement in data sharing and NEHR access to reduce the risk of further data breaches; and
(c) Assess if there are patterns that signal a larger-scale attack, and thus take prompt action to protect the integrity of Singapore's healthcare system.

62. Entities will be required to notify MOH of:

(a) Any data breach[3] that (i) results in, or is likely to result in, significant harm to any individual to whom any health information affected by a data breach relates; or (ii) is of a significant scale, i.e., 500 or more individuals affected. This threshold is aligned with PDPA's data breach notification criteria.
(b) Any cybersecurity incident[4] that happens to a computer or computer system that is (i) in the control of the entity; and (ii) contains health information or communicates with another computer or computer system containing health information.

63. Requirements:

(a) Once an entity has reasons to believe that a data breach or cybersecurity incident has occurred, the entity must assess in an expeditious manner whether the incident is a notifiable incident. Where an incident meets the criteria for notifying MOH, the entity must notify MOH within two hours, after the entity has either (i) credible grounds to believe that a prescribed cybersecurity incident has occurred, or (ii) assessed that a data breach (including unauthorised NEHR access) is notifiable. The duration of 2 hours allows MOH to take prompt action for severe cyber-attacks that may cause serious harm to patients.
(b) Entities will be required to notify affected individuals without undue delay if the incident is likely to result in significant harm to them. For the purposes of the Bill, any **sensitive health information**, if compromised in an incident, is considered as likely to result in significant harm to an individual.

[3] For the purpose of notification to MOH, "Data breach" refers to any unauthorised access, collection, use, disclosure, copying, modification, disposal of health information, or loss of any storage medium or device on which health information is stored.

[4] For the purpose of notification to MOH, "Cybersecurity incident" refers to (i) any unauthorised hacking of the computer or computer system to gain unauthorised access to or control, (ii) installation or execution of unauthorised software or computer code of a malicious nature, (iii) unauthorised interception of communication, or (iv) unauthorised act that adversely affects the availability or operability of the entity's computer or computer system.

(c) Entities must submit an incident report providing further details of the incident (including its cause and impact) 14 days after the initial incident notification to MOH.

This will help maintain public trust in the healthcare sector's ability to share health information securely. Unreasonable delay in assessing or notifying the incident will be a breach of the incident notification requirement.

64. To be clear, the following events are not reportable to MOH under the Bill:

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

Requirements for Data Intermediaries

65. The Bill will impose obligations for data intermediaries. 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.

66. Data intermediaries are defined under the Bill as organisations that process health information on behalf of an entity, but do not include an employee of that healthcare provider, for purposes prescribed under the Bill. This includes:

(a) Organisations providing health information processing services for the purpose of the healthcare provider accessing or contributing to the NEHR (e.g., CMS vendors); and
(b) Organisations providing a health information processing service to a care provider under the Bill, and which involves the disclosure and receiving of health information enabled under HIB as a prescribed use case.

67. 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.

68. Four obligations will be imposed on data intermediaries under the Bill:

A. Cybersecurity and Data Protection. A data intermediary must make reasonable security arrangements to protect the entity's health information and computer systems containing health information that are in the data intermediary's possession or control.

B Retention Limitation. For records containing health information, the data intermediary must retain the records for the specified time period based on the entity's legal or business purposes, and take reasonable care in the disposal or destruction of the records once the entity no longer has a legal or business need to retain them.

C. Incident Notification. Upon the discovery of a cybersecurity incident or data breach, data intermediaries are required to inform the entity of the incident without undue delay if the incident (1) affects the services provided to the entity, or (2) involves health information of the entity.

D. Data Portability. The fidelity of health records should be upkept when data is transferred from one data intermediary to another, but these are typically outside the control of the entity. As such, the data portability requirements are intended to establish minimum requirements with regard to data migration, in order to uphold data portability. This includes establishing the format of the data to be exported, the responsibilities for the "incoming" and "outgoing" data intermediaries, as well as the entity's.

69. Delineation of accountability between the data intermediary and entity: Entities, not the intermediaries, will have ultimate responsibility for the entity's compliance to the Bill requirements. The entity under the Bill should use only data intermediaries which provide sufficient safeguards and assurance that their processing of health information will meet the HIB requirements. The entity's responsibilities involve making clear in its contract the scope of work that the data intermediary is to perform on its behalf, and for what purposes.

Application of Requirements

Cyber and Data Security Requirements

70. The HIB data security requirements will supersede the Personal Data Protection Act (PDPA)'s Protection Obligation. While PDPA has established sector-agnostic data protection obligations (i.e., reasonable security arrangements for the processing of personal data) for enterprises to abide by, there is a need for specific data security requirements (e.g., proper storage, reproduction, and transmission of data to prevent unauthorised access or loss of patient data) for healthcare providers under the HIB to better secure the sharing and use of health information.

71. The HIB cybersecurity requirements will not supersede the Cybersecurity Act ("CS Act") in relation to the regulation of critical information infrastructure ("CII") in the healthcare sector.

Incident Notification Requirement

72. PDPC provides a baseline data breach notification requirement applicable to all private sector organisations in Singapore, while the Bill's incident notification requirements are tailored to the healthcare sector's needs. Therefore, the Bill will supersede the PDPA in relation to the notification of health information breaches affecting a healthcare provider. Data breaches that are reported to MOH do not need to be reported to PDPC. Nonetheless, MOH and PDPC will practice a "no-wrong-door" policy should breaches be reported to the incorrect agency. The agencies will streamline reporting requirements across the various legislations.

73. However, for healthcare CII owners, the Bill will not supersede the CS Act in relation to the reporting of cybersecurity incidents.

VII. Enforcement of the Bill

While the Bill enables health information to be shared securely and for patient care purposes, non-compliance with the security requirements in the Bill will result in strict penalties. The Bill also provides powers to ensure requirements are complied with.

General Powers

74. The Bill will accord MOH powers to issue directions for entities to rectify non-compliances with the Bill. Such powers include: stopping the unauthorised access and collection of 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 complying with the cybersecurity and data security requirements.

75. 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.

76. MOH will continue to work with CSA and PDPC to investigate more complex cases involving cybersecurity incidents and data breaches occurring in entities, and mete out the appropriate penalties for non-compliances accordingly under the various Acts.

Emergency Powers

77. The Bill accords MOH a set of emergency powers in relation to the healthcare sector, to perform remediation measures involving health information in severe situations. The powers can be invoked in any situation where the unauthorised disclosure, modification, destruction, or unavailability of health information have the potential to cause:

(a) Serious and irreversible harm to patient safety and welfare, such as permanent disability and death;
(b) Serious and imminent threat to the public health of Singapore; and
(c) Serious disruption to healthcare service provision and capacity at the national level.

78. The proposed emergency powers will allow the Minister (or for the Minister to authorise an officer) to direct an entity to remediate or mitigate the situation or threat, within a prescribed time period. The entity may be directed to take measure in relation to the processing of health information, to address, stop or prevent further escalation of the situation. This could include directing the entity to:

(a) Provide necessary information to MOH where needed or when requested for;

(b) Take action, or instruct other organisations or individuals to take action pertaining to the collection, storage, transmission, modification, or destruction of health information.

79. Examples of how such powers could be applied include directing a healthcare provider to:

(a) Isolate certain data types from access on their physical or electronic records due to an incident rendering it untrustworthy.
(b) Collect health information for the purpose of healthcare service provision, if the original data have been destructed or modified beyond recovery, and the lack of such information could cause severe injury or national-level capacity issues.
(c) Re-validate, and then re-contribute any information that may have been modified or contributed in a way that results in the information in the NEHR being erroneous, and such information could potentially bring about significant harm to the patient's health or treatment.

80. Given the expanded scale of data sharing under the Bill, and the dangers that corrupted or unavailable health information could create for patients, the emergency powers would allow MOH to take immediate action to protect patient safety and the availability of the healthcare system and services in the event of emergencies. There will be an internal governance process within MOH to ensure that the powers are exercised responsibly and in accordance with the Bill, and only by qualified persons.

Offences and Penalties Framework

81. The proposed penalty framework seeks to secure ongoing compliance by entities, and provide sufficient deterrence for both individuals and organisations. This will ensure appropriate measures are in place to safeguard patients' health information, and prevent the unauthorised disclosure and misuse of health information. The offences and penalties will be aligned to that of relevant Acts, such as the Computer Misuse Act, PDPA, and CS Act.

82. MOH will have the power to issue orders for entities to rectify non-compliances with the Bill. For non-compliances that exceed a certain scale and severity, MOH will have the power to require the organisation to pay a financial penalty 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.

83. MOH understands that entities may be victims of cybersecurity or data breaches. The penalties are not intended to penalise entities solely based on an actualised cybersecurity incident or data breach. Instead, the penalties will only be levied in cases of non-compliance with instructions and HIB requirements, or if the entity wilfully refuses to provide information or cooperate with MOH.

Penalties for Individuals

84. Besides 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:

(a) Unauthorised disclosure, or conduct causing the disclosure of health information;
(b) Unauthorised use of health information to obtain a gain, or cause harm or loss to another person; and/or
(c) Re-identification of anonymised health information.

85. 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. Given that the accountability of cyber and data security for prescribed entities will fall under the HIB's scope, this allows MOH to have a streamlined approach for the enforcement of all non-compliances to health information use and sharing. These offences do not detract from the policy position to hold organisations 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 sanctions.

Summary of Compliance Approach

86. 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, for example:

(a) Unauthorised access to a patient's NEHR records, as detected by the individual's HealthHub records;
(b) Unauthorised disclosure and sharing of a patient's health information when the patient has placed restrictions on the sharing of his/her data;
(c) Suspected breach of the patient's health information.

Annex B: Proposed List of Data Types to be Contributed by Healthcare Licensees to the NEHR

Licensable Healthcare Service (LHS)	Blood Banking	Clinical Laboratory	Cord Blood Banking	Emergency Ambulance	Medical Transport	Radiological	Acute Hospital	Community Hospital	Ambulatory Surgical Centre	Assisted Reproduction	Outpatient Dental	Outpatient Medical	Outpatient Renal Dialysis	Human Tissue Banking	Nuclear Medicine	Nursing Home	Preventive Health
Patient Demographics	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
Cardiac Reports (Cath Lab/2D Echos)	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v
Dental Note (including dental chart - Odontogram)	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v
Discharge Summary (inpatient)	NA	NA	NA	NA	NA	NA	M	M	M	M	NA	NA	NA	NA	NA	M	NA
Dispensed Medications (Discharge & Outpatient, excludes meds orderd for in-flight admission administration)	NA	NA	NA	M	M	M	M	M	M	M	M	M	M	NA	M	M	M
Drug Allergy/Adverse Drug Reactions	NA	NA	NA	M	M	M	M	M	M	M	M	M	M	NA	M	M	M

Licensable Healthcare Service (LHS)	Blood Banking	Clinical Laboratory	Cord Blood Banking	Emergency Ambulance	Medical Transport	Radiological	Acute Hospital	Community Hospital	Ambulatory Surgical Centre	Assisted Reproduction	Outpatient Dental	Outpatient Medical	Outpatient Renal Dialysis	Human Tissue Banking	Nuclear Medicine	Nursing Home	Preventive Health
ED Notes (ED Summary)	NA	NA	NA	NA	NA	NA	M	NA	NA	NA	NA	NA	NA	NA	NA	NA	NA
Events	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M	M
Immunisation	NA	NA	NA	NA	NA	NA	M	M	M	NA	NA	M	M	NA	NA	M	M
Laboratory	M	M	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v	M	r/v	r/v
Ordered (Prescribed) Medications (Discharge & Outpatient, excludes meds ordered for in-flight admission administration)	NA	NA	NA	M	M	M	M	M	M	M	M	M	M	NA	M	M	M
OT Notes/Procedure Notes (TOSP Table 1A and above)	NA	NA	NA	M	M	M	M	M	M	M	M	M	M	NA	M	NA	NA
Patient Medication List/ Medication Reconciliation Document	NA	NA	NA	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v

Licensable Healthcare Service (LHS)	Blood Banking	Clinical Laboratory	Cord Blood Banking	Emergency Ambulance	Medical Transport	Radiological	Acute Hospital	Community Hospital	Ambulatory Surgical Centre	Assisted Reproduction	Outpatient Dental	Outpatient Medical	Outpatient Renal Dialysis	Human Tissue Banking	Nuclear Medicine	Nursing Home	Preventive Health
Patient Problem List (in SNOMED)	NA	NA	NA	r/v	r/v	r/v	**r/v**	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v
Imaging/Radiology Reports	NA	NA	NA	NA	NA	M	NA	NA	NA	NA	NA	NA	NA	NA	M	NA	NA
Radiology Images	NA	NA	NA	NA	NA	r/v	NA	NA	NA	NA	r/v	NA	NA	NA	r/v	NA	NA
Referral Note	NA	NA	NA	M	NA	NA	M	M	M	M	M	M	M	NA	NA	M	M
Visit Diagnosis (In SNOMED)	NA	NA	NA	NA	NA	NA	M	M	M	r/v	M	M	M	NA	M	M	M
Ophthalmology Reports (DRP)	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v	r/v

Legend

M	Licensees are required to submit the data types if they generate such information
r/v	Contribution of data type is under review by MOH
NA	Licensees are not required to contribute such data

Annex C: Proposed Details of Unified Cyber and Data Security Requirements

Cybersecurity
Asset Entities must establish and implement mechanisms and processes to: a) identify and maintain oversight of all computers and computer systems assets under its control; and b) monitor, detect and manage the cybersecurity vulnerabilities of these assets.
Secure – *Access control, secure configuration, and software updates* Entities must ensure adequate safeguards to prevent and detect access by unauthorised personnel, activities or devices to the entities' computers and computer systems. Entities must ensure that protocols are in place to perform periodic user access review verifying that users and their accounts are granted the least extent of access necessary to perform their required functions. Entities must make reasonable arrangements to protect against the exploitation of security vulnerabilities by: a) securing the configurations of their computers and computer systems; and b) performing regular security updates and patching to address critical and known security vulnerabilities.
Data Security
Identify – *data security classification, marking requirements* Entities must ensure health information in its possession or under its control is appropriately classified according to the data's sensitivity. Entities must establish and implement practices to store health information in a secure manner. The security safeguards taken to secure the health information must be commensurate with the data sensitivity level and the security risk of a data breach.
Access – *authorised users* Entities must put in place protocols to ensure that users are granted the least extent of access to health information necessary to perform their required functions. The protocols must include processes to periodically review, and if necessary, change or revoke the users' access rights to health information.
Secure – *storage, reproduction, and conveyance requirements*

Entities must put in place processes to ensure that health information in its possession or under its control is transmitted (via mailing or electronic transmission) or conveyed (via a conveyance to another physical location) securely.

Common Cyber & Data Requirements

Outsourcing & Vendor Management

Where entities:

a) engage or use a third-party software, device or system, the entity must put in place policies and practices to ensure the confidentiality, integrity and availability of the entity's information processed on these software, devices, and systems; and

b) engage a third-party vendor in the management of the entity's computer systems (e.g., outsourcing of IT services to a vendor) or the processing of health information (e.g., data entry), the entity must implement processes and protocols to ensure the entity's policies and practices to manage cybersecurity risks and safeguard health information assets are adhered by the vendors.

Incident Response

Entities must establish an incident management framework to detect, respond to, mitigate, and recover from health information breaches and cybersecurity incidents ("incidents"). The framework must cover:

a) roles and responsibilities of personnel involved in the incident response process; and

b) procedures to detect, respond, and recover from common incident scenarios (e.g., ransomware, DDoS attacks).

Retention Limitation

Entities must dispose or destruct health information that they possess in a proper manner, once retention is no longer necessary for any legal or business purposes.

Backup and Emergency Planning for Contingency

Entities must establish and implement a backup and restoration plan to ensure that its critical systems can be restored effectively, and critical data can be recovered in the event of a system disruption or failure, cybersecurity incident, or the loss, corruption or unavailability of health information.

Entities must perform periodic backups at a frequency that is commensurate with the entity's operational requirements.

Review Security & Internal Audit Requirements

Entities must perform regular checks to ensure compliance and minimise the risks of cyber-attacks.
Compliance by Personnel Entities must ensure that each personnel who handles the entity's IT systems and health information is aware of: a) the personnel's role in maintaining the security of the health information and IT systems; and b) all security safeguards to ensure compliance with the HIB requirements, and complies with the safeguards.

Annex D: List of Existing Support Schemes for Entities

Existing Support Schemes	Description
IMDA/ESG Productivity Solutions Grant	For cybersecurity solutions, eligible SMEs may consider adopting pre-approved cybersecurity solutions under the Productivity Solutions Grant (PSG) that meet your needs. IMDA maintains a list of pre-approved cybersecurity solutions including managed detection and response, unified threat management, and endpoint protection platforms. These solutions have been market-tested and are meant for quick adoption to improve productivity. The PSG provides up to 50% support for eligible companies, with an annual grant cap of S$30,000.
IMDA Chief Technology Officer-as-a-Service (CTO-aaS)	The Chief Technology Officer (CTO)-as-a-service (CTO-aaS) scheme offered by the Infocomm Media Development Authority (IMDA) enables SMEs in Singapore 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.
CSA Cybersecurity Health Plan	Eligible Small and Medium- sized Enterprises (SMEs) can subscribe to the CSA's Cybersecurity Health Plan – a scheme with up to 70% co-funding support upon signing up with the CISO-as-a-Service (CISOaaS) cybersecurity consultants onboarded by CSA. 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 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.
NCSS Tech-and-Go! Scheme	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.

Early Contribution Incentive (ECI)	The Early Contribution Incentive (ECI) is developed to support private healthcare licensees in contributing data to the NEHR. It is a one-time funding support scheme designed to help defray cost of upgrading and/or integrating the IT system with the NEHR for data contribution. The application process will take place in two phases. Phase 1 was rolled out in December 2022 for hospitals, clinical laboratories, radiological laboratories and general practitioners. Phase 2 will be rolled out for the remaining licensees in 2023/2024.
GP IT Enablement Grant	The GP IT Enablement Grant is a one-off grant that supports GP clinics to adopt a suitable Clinic Management System (CMS) under the CMS Tiering Framework for Primary Care. GP clinics can apply for funding support of $10,000 (for Healthier SG clinics) or $3,000 (for non-Healthier SG clinics).