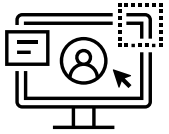
What does this mean for... Data Intermediaries



An organisation is a data intermediary if it processes health information on behalf of a healthcare provider for HIB's prescribed purposes.

Vendors for clinical management systems that access and contribute health information to the National Electronic Health Record

NEHR
National Electronic Health Record Singapore

IT services vendors and **software providers** that process health information obtained from the HIB's data sharing use cases

DATA SHARING
Of Health Information in other health record systems

Delineation of responsibility between the healthcare provider and data intermediary should be spelt out in the contractual agreement between the healthcare provider and data intermediary. This should include contractual clauses to ensure that the data intermediary's scope of work and level of responsibilities are clear.

The data intermediary and healthcare providers should agree on the following:

1. **Indicate if the health information being processed by the data intermediary are related to purposes prescribed under the Bill, and the related obligations under HIB.**
2. **Set out the duration, nature, and purpose of the health information processing.**
3. **Set out requirements for the data intermediary, and steps to be taken in the event of an incident (e.g. cybersecurity attack, data breach)**

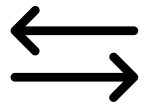
The requirements imposed on data intermediaries are generally similar to those prescribed under the Personal Data Protection Act, and broadly aligned with international standards regarding the delineation of accountability between the data controller and data processor.

A data intermediary is required to, under the Health Information Bill:

Data Protection: Make reasonable security arrangements (e.g. allow for encryption of sensitive data, access control policies based on principle of least privilege) to protect health information that it possesses or controls.

Retention Limitation: Dispose all records containing health information, once the healthcare provider no longer has any legal or business requirements to retain it.

Incident Notification: Inform the healthcare provider without undue delay once the data intermediary discovers a cybersecurity incident or data breach affecting the healthcare provider's health information.



Data Portability: Maintain health information that it processes in a format such that the data can be easily moved, copied or transferred should the healthcare provider decides to switch to another vendor.

There will be penalties for non-compliance to the requirements.