CHAPTER 8

STANDING DATABASES

8.1 Standing Databases

8.2 Responsibilities of Custodians

8.3 Consent for the Storage of Data for Future Use

8.4 Data Management

8.1 Standing Databases

I. Definitions

Standing Database (SDB) - Contains electronic data stored as a potential resource for future research.

Owner The institution / cluster is the owner of the database set up by their staff member for the purposes of future research.

Custodian Any individual appointed by the data owners to be the overall person responsible for the set-up, conduct and maintenance of a standing database.

Database Team Member Any individual member of the standing database team designated and supervised by the custodian to perform database-related activities that may or may not involve participant contact (e.g., database administrators).

Department Representative / Head of Department (DR / HOD) Endorsement to ensure traction over the collection and storage of data and that the department can adequately support the set-up, maintenance and closure of the SDB.

Institution Representative (IR) Endorsement to ensure the custodian knows the institutional and legal responsibilities and is compliant to the institution policies.

Institutional Review Board (IRB - DSRB) Acknowledgement and review to ensure that the recruitment and consent process of the participants complies with ethics requirements & regulations.

Research Data Institutional Deputy (ID) The ID is appointed by the PIC to provide an independent and timely review of standing database applications and grant approval for the establishment of standing database in his/her institution.

Research Data Secretariat (RDS) The secretariat provides support to the NHG Health Principal Person-In-Charge (PIC) to oversee cluster policies and procedures on the use and management of research data.

Principal Person-In-Charge (PIC) PIC is responsible for ensuring that all research data related activities comply with legislation, the Human Biomedical Research Act (HBRA), the Personal Data Protection Act (PDPA) and Healthtech Instruction Manual (HIM).

II. Considerations When Setting up a Standing Database (SDB)

The procedure for setting up the database and subsequent acquisition of data should be written and adhered to. This should include (but not limited to):

a. A list of names and designations of the custodians and personnel given access to the database. This "access list" should be updated regularly. Access to the database should be restricted to authorized personnel only and should be supervised closely by the appointed custodian and kept to a justifiable minimum.

b. A description of the types, sources, method of collection, storage, transfer, retention and disposal of the data.

c. Information on the consent process or justifications for a waiver of informed consent.

d. Security measures used to maintain confidentiality of data.

e. A description of the process to ensure that individual research studies utilizing data from the database will not be conducted without IRB and Institutional authorities' review.

Where there is shared ownership of a database amongst various NHG Health or Non-NHG institutions, the owners should agree upon the most suitable custodian.

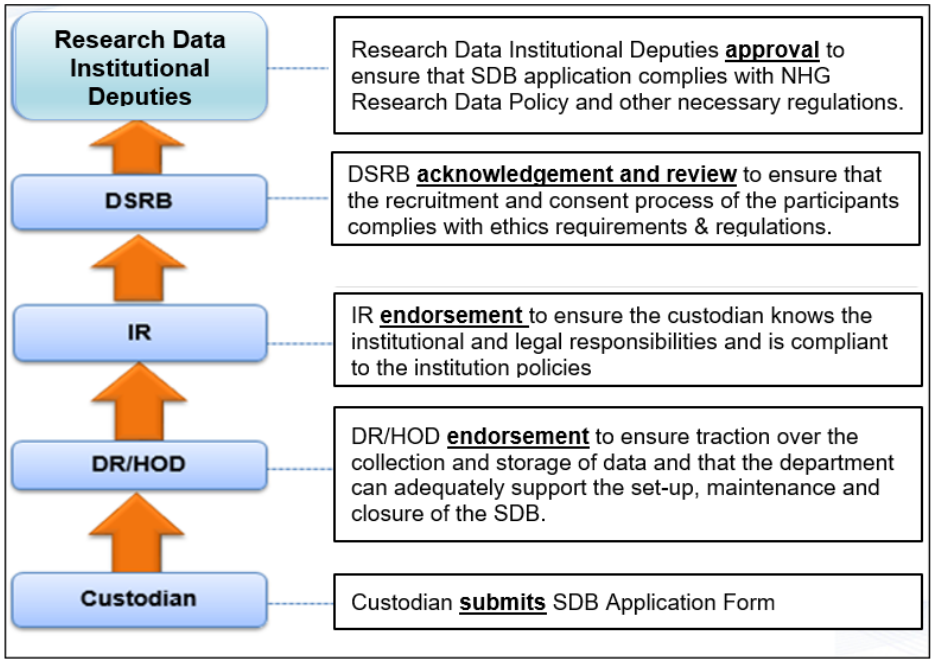
III. Registration of Standing Databases

Databases that are created with the intention of using the stored data for future research should be registered as a Standing Database (SDB). Databases which are created as part of a previous IRB approved research study that has since been completed, may be set up to store data for possible research. Such databases should be registered as a SDB upon completion of the research study. Prior permission must be sought from the relevant institutional authorities before the setting up of SDBs.

For Non-NHG Institutions: Custodians would need to adhere to their own institution requirements when setting up SDBs and are also encouraged to submit a Standing Database Application to their ID equivalent for review and approval.

For NHG Health Institutions: With effect from 01 August 2020, all new SDBs and amendments must be approved by NHG Health Research Data Institutional Deputies (IDs), before proceeding with SDB activities. Figure 5 below reflects the review process for NHG Health SDB applications.

Figure 5: NHG Health Standing Database Applications Review Process



The custodian and database team members must also disclose any real or apparent conflict of interest in the application form to the ID.

8.2 Responsibilities of Custodians

Custodians are responsible for the proper collection, use and disclosure of data, including the release of data from these standing databases for research. Responsibilities of a Custodian include (but not limited to):

a. The custodian must be in the permanent employment of an institution under NHG Health. Ensure he / she is qualified by education, training and experience to assume responsibility of managing a standing database. He/she must also maintain an up-to-date curriculum vitae. For NHG Health custodians, he / she must be in the permanent employment of an institution under NHG Health.

b. Maintain a list of persons to whom he/she has delegated significant database related responsibilities.

c. Appoint adequate qualified staff to properly manage the standing database.

d. Ensure that all persons assisting with the conduct of the database are adequately informed about the collection, use and disclosure of the data as well their duties related to the management of the standing database.

e. Disclosure of any potential conflict of interest between, Custodian and / or Data Team Members with the participants in the application of the Standing Database or during the duration of the Standing Database.

f. Ensure compliance with Standing Database Application approved / acknowledged by applicable parties (e.g., IR, IRB, ID). Deviations from or changes of the project should not be implemented without prior review and documented approval / acknowledgement applicable parties.

g. Manage, access and utilize data in a manner that is consistent with their institutional policies and applicable regulatory requirements.

h. Ensure recruitment of participants is in a fair and equitable manner.

i. Ensure that informed consent is obtained from potential participants prior to their enrollment into the standing database, unless consent is waived by applicable parties (e.g. IRB). The most current consent document must be used to obtain consent.

j. Maintain all relevant documents and allow audits / inspects of such records from applicable parties.

k. Ensure accuracy and completeness of data in all case report forms and all standing database related documents.

l. Ensure that applicable approvals are obtained prior to allowing a third party to access / utilize the standing database.

m. If the custodian is going away for a long time, the standing database should be formally transferred to another custodian. Should the custodian be leaving the employment of the institution, another employee should be appointed as the new custodian by the institution, as the custodian does not possess any ownership of the database. The incoming individual should be qualified and assumes all the responsibilities as the custodian.

n. The custodian should inform the owner(s) and relevant parties (e.g., NHG Health ID) when the database has ceased to be useful and is therefore decommissioned.

For Non-NHG Institutions: Custodians would need to adhere to their own institution requirements for standing database maintenance.

For NHG Health Institutions: After ID's initial approval, the custodian should continue to comply with the following:

a. Submit standing database status reports to the ID before the expiry date of the approval.

b. Report non-compliances, deviations as well as suspected data breaches to ID and other authorities, where relevant, in accordance with institutional requirements.

c. Custodians who will be away for more than 6 months would need to formally transfer the standing database to another custodian. This change should be reviewed and approved by the ID.

NHG Health custodians should refer the **NHG Health Research Data Policy** and applicable institution requirements for more information on how research data should be managed.

8.3 Consent for the Storage of Data for Future Research

INFORMED CONSENT - For databases that are intended for use in possible future research (regardless of whether the primary function is for research or not), informed consent from participants should be obtained. Custodians are to ensure that all required consent elements are present in the Informed Consent Form provided to participants.

If the stored data is planned to be used in future studies regulated by the Human Biomedical Research Act (HBRA), the Informed Consent Form must contain all the Section 12 (1) appropriate consent elements of the HBRA.

WAIVER OF INFORMED CONSENT– In certain circumstances the requirement to obtain informed consent may be waived. The custodian must be able to justify the criteria for a waiver of informed consent for the standing database in their submissions to IRB/ID.

For more information on informed consent, please refer to Chapter 5 Informed Consent.

8.4 Data Management

8.4.1 Confidentiality

Harm that may occur because of database activities are mostly related to threats to privacy and breaches in confidentiality. There should be policies and procedures in place to ensure adequate protections for privacy and maintenance of confidentiality. Such procedures should regularly be reinforced by the appointed custodian to all personnel who have been granted access to the standing database. Owners and appointed custodians of standing databases may undertake regular internal audits to monitor compliance with these guidelines and to ensure that there are adequate protections put in force.

The confidentiality of the private information contained in the databases is primarily the responsibility of their respective custodians. Custodians need to put in place data security features to prevent and monitor regularly for unauthorized access to the database. Such precautions could range from structural or IT-based solutions features (e.g., installation of firewalls, encryption or password protection) to organizational and administrative measures (e.g., regular audits).

Databases should be stored in secured corporate issued computers / laptops / storage media. These computers/laptops/storage media must be password protected, and stored under lock and key (e.g., in a locked cupboard/ office). There should be scheduled changes (e.g., at least every 6 months) of passwords.

Owners and custodians are responsible for taking active steps to ensure that all staff who are given access to the database as part of their work, maintain the confidentiality at all times. They must also ensure compliance with their respective institutions' research data management policies (e.g., NHG Health Research Data Policy).

8.4.2 Utilisation of Stored Data

Each subsequent research study (including studies initiated by the custodian and all staff listed in the "access list") utilising any standing database will require prior approval from IRB before study initiation. The concurrence of the custodian should also be obtained.

Depending on the nature of the study, IRB and / or ID will determine if access to the standing database may require additional consent. Some considerations by the IRB will include whether any patient contact is proposed, the practicability of getting informed consent for the research and whether the data extracted and used for the research will be de-identified or aggregated etc.

In general, recipients of the data should not be provided with identifiable information or to information through which identities of patients or subjects may be readily ascertained.

8.4.3 Disposal of Stored Data

When the database is no longer required (with agreement from custodian, data owner, and applicable parties), all data and identifying links must be destroyed according to institutional disposal policies. Documentation of destruction (e.g., by whom and when was the destruction) should also be maintained.

The actual destruction of Classified materials shall be witnessed by appropriate Entity personnel, especially where Classified data may be viewed by unauthorised individuals during the disposal process[1].

Documentation of the Classified material, destruction process, and declaration by the destruction personnel and witness shall be kept for a period of at least 3 years.

8.4.4 Retention of Research Data

Study teams must retain research data for a minimum period. Currently, the minimum retention period of research data is 6 years. Study teams may retain research data for a longer period, where it is specifically indicated.

Should the owner deem it necessary to archive the database for future reference, the owner should continue to comply with the guidelines for the storage of data. The owner shall be responsible for the safekeeping of archived database.

8.4.5 References and Further Reading

For Non-NHG institutions: Please approach your respective institutions on their research data policies.

For NHG Health institutions: NHG Health Custodians should adhere to the **NHG Research Data Policy** and other applicable institutional requirements to ensure that their standing database is appropriately managed.