DATA RETENTION, DESTRUCTION, AND RESTORATION

– Policy –

1. PURPOSE

1.1 This Policy describes the secure retention, destruction, and restoration (where applicable) of Master Data Set, Project Data Sets, Data Backups, and Storage of Administrative Data transferred to and held in the secure custody of the New Brunswick Institute for Research, Data and Training (NB-IRDT) as a Research Data Centre as defined in the New Brunswick *Personal Health Information Privacy and Access Act, SNB 2009, c P-7.05* *(PHIPAA)* and New Brunswick *Right to Information and Protection of Privacy Act*, SNB 2009, c R-10.6 (RTIPPA).

2. SCOPE

2.1 This Policy applies to all Personal Information and Personal Health Information held in the custody of NB-IRDT inclusive of: Master Data Set; Project Data Sets and Research Product Data (i.e., project specific External Data Sets; and data that has been backed-up or stored.

2.2 This Policy applies to all NB-IRDT lines of business including Data Access and Use, and Information Manager services.

2.3 This Policy does not apply to the business and operational records of NB-IRDT that are subject to the records management practices of the University of New Brunswick (UNB) or a government body.

3. DEFINITIONS

3.1 *Approved Data User(s):* Individuals, such as NB-IRDT Employees, researchers, students, and government employees, who have been issued an electronic identification access card, personal identification number, and project access account following the approval of access according to all relevant NB-IRDT procedures, including a Criminal Record Check (CRC).

3.2 *Archiving of Data (Data Archive)*: The long-term retention of selected data with firm start and end dates that are established in cooperation with partners through Data Sharing Agreements prior to any receipt of data. Dates of archived retention are outlined in the NB-IRDT Data Retention and Destruction Schedule and/or Data Sharing Agreements, and Data Retention Schedules.

3.3 *Backup of Data (Data Backup)*: The regular (e.g., daily, weekly,) secure copying and storing of data that would facilitate any necessary rapid restoration of data and minimize the impact of failures due to human error or disaster.

3.4 *Custodian:* As defined in the PHIPAA, an individual or organization that collects, maintains, or uses personal health information for the purpose of providing or assisting in the provision of health care, treatment, the planning, and management of the health care system, or delivering a government program or service.

3.5 *Data Business Owner:* The entity holding legal rights and control over a Data Set(s) and its variables. In the context of a Data Sharing Agreement, this is the entity (e.g., Custodian, Public Body) who has signed the Data Sharing Agreement and who has shared/disclosed a Master Data Set with/to NB-IRDT.

3.6 *Data Platform:* Comprehensive repository that holds Pseudonymous Administrative Data available by Data Access Request.

3.7 *Data Retention and Destruction Schedules:* Schedules that specify the beginning and end dates for the retention of the data inclusive of any requirements from the owner of the data or specified in any Data Sharing Agreements.

3.8 *Data Set(s):* A collection of related, but distinct data that can be accessed individually, in combination, or managed as a whole. Often organized in rows and columns where each column of the table represents a particular variable, and each row corresponds to a given member of the Data Set in question. For NB-IRDT purposes, rows often contain individual records (such as a person's visit to hospital), while columns contain relevant variables.

3.9 *External Data Sets*: Data Sets that are transferred under Data Sharing Agreements with Data Business Owners/Custodians for use with a specified approved project. Data Sets are returned to the Data Business Owner/Custodian on Project Closure.

3.10 *Information Manager*: An individual or organization that, on behalf of a Custodian, processes, stores, retrieves, archives or disposes of Personal Information and/or Personal Health Information; de-identifies or otherwise transforms Personal Information and/or Personal Health Information; and/or, provides information management or information technology service.

3.11 *Information Manager Data (at NB-IRDT):* Pseudonymous data provided by a Data Business Owner/Custodian and used for that Data Business Owner's purposes. At the NB-IRDT Hub Location, it is stored on a separate partition on the server, which is not part of the Data Platform.

3.12 *Master Data Set (Master Data):* The original Data Set received by NB-IRDT from a Data Business Owner/Custodian, provided on an encrypted media transfer device.

3.13 *New Brunswick Institute for Research, Data and Training (NB-IRDT)*: A Research Data Centre as defined in RTIPPA and PHIPAA. Like other Research Data Centres, NB-IRDT has the authority to compile and link Personal Information or Personal Health Information for the purposes of research, analysis, or evidence-based decision-making. NB-IRDT has three locations, with the Hub located in Fredericton, and Satellite Sites located in Saint John and Moncton. These facilities are situated on the University of New Brunswick (Fredericton) campus (Keirstead Hall, 38 Dineen Drive; Units 316, 317, and 317-A); on the Saint John campus (Hazen Hall, 93-97 Tucker Park Road; Unit 339); and, on the Université de Moncton campus (Bibliothèque Champlain, 415 avenue de l'Université; salle 031).

3.14 *Personal Health Information*: As defined in the PHIPAA, information about an individual in oral or recorded form if the information:

- relates to the individual's physical or mental health, family history or health care history, including genetic information about the individual;
- is the individual's registration information, including the Medicare number of the individual;
- relates to the provision of health care to the individual;
- relates to information about payments or eligibility for health care in respect of the individual, or eligibility for coverage for health care in respect of the individual;
- relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any body part or bodily substance;
- identifies the individual's substitute decision maker; and/or
- identifies an individual's health care provider.

3.15 *Personal Information*: As defined in the RTIPPA, means oral or recorded identifying information related to an individual, including, but not limited to:

- the individual's name;
- the individual's home address, electronic mail address, home telephone or facsimile number;
- information about the individual's age, gender, sexual orientation, marital status, or family status;

- information about the individual's ancestry, race, colour, nationality, or national or ethnic origin;
- information about the individual's religion, religious belief(s), religious association or activity, or creed;
- Personal Health Information about the individual;
- the individual's blood type, fingerprints, or other hereditary characteristics;
- information about the individual's political belief, association, or activity;
- information about the individual's education and employment or occupation or educational, employment or occupational history;
    - information about the individual's source of income or financial circumstances, activities, or history;
    - information about the individual's criminal history, including regulatory offences;
    - the individual's own personal views or opinions, except if they are about another person;
    - the views or opinions expressed about the individual by another person; and/or,
    - an identifying number, symbol, or other particular assigned to the individual.

3.16 *Project Closure (Research Project Closure)*: The procedures and actions to ensure NB-IRDT's responsibilities are met in terms of removing Approved Data Users access to the Secure Research Environment and/or Project Data Sets, and Project Data are moved to secure storage immediately following a Project End Date.

3.17 *Project Data Set(s)*: Data prepared for a specific project and stored in a project folder, which consists only of information approved for a specific research project. Project Data Sets are generated by the NB-IRDT Database Administrator who extracts, and links approved variables from platform and External Data Sets, including public databases (e.g., Census profiles, and researcher's own databases).

3.18 *Project End Date (Research Project End Date)*: The date project work ceases and Approved Data Users access to the Secure Research Environment and/or a Project Data Set are removed. This date coincides with one or more of the following: the Research Ethics Board expiration date, the end date set in the grant for evaluation work, the end date set in the Data Access Agreement (DAA)/contract, or, if prior to the approved end date on DAA, upon notice of project completion by the Principal Investigator.

3.19 *Project Start Date (Research Project Start Date)*: The date on which project work may begin and Approved Data Users have access to the Secure Research Environment and/or a Project Data Set. This date coincides with the signature date of the Data Access Agreement for an approved research project.

3.20 *Pseudonymous Data*: Information from which direct identifiers (e.g., name, Medicare numbers, social insurance number) have been eliminated or transformed, but indirect identifiers (e.g., date a service was accessed, medical diagnosis, length of hospital stay, occupation, level of education) remain intact.

3.21 *Research Data Centre (RDC)*: A public body that compiles and links personal information and/or personal health information for the purposes of research, analysis, or evidence-based decision-making.

3.22 *Research Product Data*: Research data output from an approved research project.

3.23 *Securely Destroyed*: Data that is destroyed in such a manner that reconstruction is not reasonably foreseeable in the circumstances.

3.24 *Secure Research Environment*: The infrastructure housing NB-IRDT data resources and equipment for accessing resources. The facilities are located on the University of New Brunswick (Fredericton) campus (Keirstead Hall, 38 Dineen Drive; Units 316, 317, and 317-A); on the Saint John campus (Hazen Hall, 93-97 Tucker Park Road; Unit 339); and, on the Université de Moncton campus (Bibliothèque Champlain, 415 avenue de l'Université; salle 031). The buildings housing these facilities are under respective campus security surveillance.

3.25 *Storage of Data*: The long-term retention of selected data following the NB-IRDT Data Retention and Disposition Schedule and/or Data Sharing Agreements identifying both the length of storage retention and disposition method of data with set start and end dates.

4. POLICY STATEMENTS

4.1 General privacy principles and obligations under PHIPAA require that Personal Information and Personal Health Information be retained only as long as necessary for the fulfillment of the research or Data Curation purpose. RTIPPA and PHIPAA require that all Custodians and their Agents have a written Retention Schedule for Personal Information and Personal Health Information that includes:

4.1.1 All legitimate purposes for retaining the information; and,

4.1.2 The retention period and destruction schedules associated with each purpose.

4.2 Data received from Data Business Owner/Custodian for Platform development or Information Manager responsibilities, are retained, and Securely Destroyed in accordance with the appropriate Data Sharing Agreements. NB-IRDT records the dates of receipt of such data. The data are retained until they become obsolete, or the terms and conditions of the appropriate Data Sharing Agreement have been met.

4.3 Complete Project Data Sets are stored on the NB-IRDT secure server for a period of three (3) years immediately following the Project End Date. Three (3) years is sufficient time for researchers to make revisions to academic papers or other reports for Dissemination as required as part of a peer review process for publication.

4.4 Project specific syntax, coding, etc., will be retained for an additional seven (7) years following the three (3) years of Project Data Sets retention.

4.5 All data in the secure custody of NB-IRDT is in keeping with the *NB-IRDT Record Retention and Destruction Schedule*.

4.6 Project Data Sets held in secure storage may only be accessed with the approval of the UNB Fredericton Research Ethics Board and the Data Research Committee for the purpose of project revision or extension.

4.7 The NB-IRDT computer systems are backed up regularly for the protection of NB-IRDT work products and restoration in the case of disaster.

4.8 Restoration of data from Data Backups or Archives will only be done for disaster recovery or if required for specific projects.

4.9 Data will only be restored from Data Backup or Archives with the approval of the NB-IRDT Director.

5. PROCEDURES

5.1 Data Retention on Receipt of Data Sets

5.1.1 Upon receipt of encrypted media devices containing Master Data Set, the NB-IRDT Database Administrator will record the date of receipt, decrypt and upload the data to the NB-IRDT server and store the media devices in the NB-IRDT safe.

5.1.2 The media devices are retained in the safe indefinitely following terms and conditions of the Data Sharing Agreement or until they are scheduled or requested to be returned or Securely Destroyed by the Data Business Owner/Custodian.

5.2 Data Retention and Destruction at Close of Research and Information Management Projects

5.2.1 A Project End Date activates the start of Project Closure procedures.

5.2.2 The NB-IRDT Data Access Coordinator informs appropriate NB-IRDT Employees to begin their respective Project Closure procedures.

5.2.3 The NB-IRDT Database Administrator will:

- Remove access to the project folder;
- Turn off access to the folder;
- Store the project syntax and vetted results; and,
- Deactivate the user accounts associated with the project.

5.2.4 The NB-IRDT Data Transfer Coordinator, working with the NB-IRDT Database Administrator, will initiate the *Data Return to Business Owners/Custodians – Standard Operating Procedure* for Data Sets identified for return to, or destruction for, the Data Business Owner/Custodian at Project Closure.

5.2.5 The NB-IRDT Systems Administrator will:

- Remove Approved Data User Secure Research Environment access if the Approved Data User is not associated with any other active research projects;
- Zip and initiate the three (3) years retention of the complete Project Data folder (i.e., Research Product Data, project syntax, specific programming codes, etc.);
- On the scheduled Project Data folder destruction date (i.e., end of three (3) years Storage):
  - Separate project folder into a) Research Product Data and b) project syntax and specific programming codes;
  - Securely Delete the Research Product Data and related Data Backup files from the server; and,
  - Initiate seven (7) years of retention for only project syntax and project specific programming codes.
- On the scheduled project syntax destruction date (i.e., end of the seven (7) additional years of retention):
  - Securely Destroy project syntax;
  - Record all related retention and destruction activities in a shared administration folder; and,
  - Document and confirm destruction using the *NB-IRDT Certificate of Destruction* and made available to the NB-IRDT

Director, NB-IRDT Data Transfer Coordinator, NB-IRDT Privacy Officer, and the Data Business Owner/Custodian.

- Record and date all storage, archiving or destruction activities in a share folder (i.e., NB-IRDT Share Point).

6. ADMINISTRATION

6.1 Accountability

6.1.1 NB-IRDT is responsible for tracking the progress of research projects, to record the Project Start and Project End Dates, to follow the NB-IRDT Record Retention and Destruction Schedule and to follow any Project Closure requirements as set out in Data Sharing and or Data Access Agreements.

6.1.2 The NB-IRDT Database Administrator is responsible to ensure that project folder access is deactivated at Project Closure.

6.1.3 The NB-IRDT Data Transfer Coordinator is responsible to ensure that all Data Sets identified for return on Project Closure are securely returned to their rightful Data Business Owner/Custodian.

6.1.4 The NB-IRDT Systems Administrator is responsible to ensure user accounts are deactivated, Secure Research Environment access is removed as appropriate, data project retention and destruction are completed on schedule, and all activities are recorded.

6.1.5 All NB-IRDT Employees with Project Closure activities are responsible for recording Closure activities.

6.2 Monitoring, Auditing, and Reporting

6.2.1 On the first of each month, the NB-IRDT Systems Administrator will verify retained data to ensure three (3) and seven (7) year retention and destruction cycles are in keeping with set Retention Schedules. In the event that NB-IRDT is inaccessible or the NB-IRDT Systems Administrator is not available on this day, verification will take place the following business day. A report detailing the verification process has been completed is provided to the NB-IRDT Data Transfer Coordinator and Privacy Officer.

6.2.2 The NB-IRDT Research and Evaluation Manager will work with the NB-IRDT Data Access Coordinator to track the progress of research projects and inform the NB-IRDT Data Access Coordinator of any Project Closures outside of scope.

6.2.3 The NB-IRDT Data Access Coordinator maintains an exhaustive project management record including Project Start and Project End Dates. The NB-IRDT Data Access Coordinator will inform responsible NB-IRDT

staff of Project End Dates and will monitor the Project Closure process.

6.2.4 The NB-IRDT Database Administrator and NB-IRDT Data Transfer Coordinator inform the NB-IRDT Privacy Officer of all Data Sets transfers to NB--IRDT, and Data Sets returned to their Data Business Owner/Custodian.

6.2.5 The NB-IRDT Privacy Officer maintains a monthly Audit of Data Set retention, destruction, and restoration activities, informed by monthly reports submitted by the NB-IRDT Database Administrator, Systems Administrator, and Data Transfer Coordinator.

6.2.6 All NB-IRDT Employees follow the *NB-IRDT Record Retention and Destruction Schedule* and/or any unique Project Closure requirements as set out in Data Sharing and Data Access Agreements.

7. RELATED DOCUMENTS

- *NB-IRDT Standard Operating Procedure: Data Return/Destruction*
- *NB-IRDT Certificate of Destruction*
- *NB-IRDT Secure Research Environment Security Policy*
- *NB-IRDT Glossary of Data Privacy and Security Terms*
- *NB-IRDT Privacy Breach Policy*
- *NB-IRDT Record Retention and Destruction Schedule*

8. REFERENCES

- *Personal Health Information Privacy and Access Act*, SNB 2009, c P-7.05
- Right to Information and Protection of Privacy Act, SNB 2009, c R-10.6

9. DOCUMENT VERSION, REVIEW, AND APPROVAL HISTORY

Version	**Author**	**Nature of Change**		**Date**
1.0	NB-IRDT Staff	Document Creation		September 2016
Approved by		**Approval Date**	**Effective Date**	**Review Date**
Vice President (Research)		November 2016	November 2016	September 2017

Version	**Author**	**Nature of Change**		**Date**
1.1	D. Curtis Maillet	Minor Revisions		June 2017
Approved by		**Approval Date**	**Effective Date**	**Review Date**

Vice President (Research)	June 2017	June 2017	September 2018

Version	**Author**	**Nature of Change**		**Date**
2.0	D. Curtis Maillet	Major Revisions		January 2019
Approved by		**Approval Date**	**Effective Date**	**Review Date**
Vice President (Research)		November 2019	November 2019	July 2020

Version	**Author**	**Nature of Change**		**Date**
2.1	Nicholas Larade	Update to current formatting		September 2021
2.2	NB-IRDT Staff	Content review – slight grammatical & spacing changes		June 30, 2022
2.2.1	NB-IRDT Staff	Content review – slight grammatical & spacing changes		May 26, 2023
Approved by **VP Research UNB**		**Approval Date**	**Effective Date**	**Review Date**
David MaGee		July 2023	July 2023	July 2024