DATA CONFIDENTIALITY AND SECURITY

– Policy –

1. PURPOSE

1.1 This Policy outlines privacy requirements and security measures that are in place to protect data on receipt from Data Business Owners and Custodians, as well as procedures for securely storing data, and protecting Personal Information from unapproved access or Use at the New Brunswick Institute for Research, Data and Training (NB-IRDT).

1.2 Safeguards regarding the Disclosure of research findings that include NB-IRDT data are found in the *NB-IRDT Dissemination of Research Findings Policy*.

1.3 Safeguards to protect physical access to the NB-IRDT Secure Facilities are outlined in the *NB-IRDT Secure Research Environment Security Policy*.

1.4 Details of the retention and disposal of data is covered in the *NB-IRDT Record Retention and Destruction Schedule*.

1.5 Detailed procedures for: receipt, preparation, and maintenance of Data Sets; enabling Use of data for research; matching of NB-IRDT data and External Data Sets; and, Use of data for information management services are detailed in the *NB-IRDT Data Service Lines of Business.*

2. SCOPE

2.1 This Policy applies to all NB-IRDT Employees and Approved Data Users regarding the receipt and Use of data for research, information management projects, and data quality and Data Curation work.

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 *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, and the treatment,

planning, and management of the health care system, or delivering a government program or service.

3.3 *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(s) with/to NB-IRDT.

3.4 *Data Curation:* The range of data quality assurance activities and processes necessary to ensure the integrity and utility of Data Sets (e.g., validation, data dictionary development).

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

3.6 *Employee(s) (of NB-IRDT):* All full-time and part-time, continuing and term Employees currently earning wages or salaries from NB-IRDT (including the Director). Does not include independent contractors.

3.7 *Hub Location:* The NB-IRDT Fredericton location which securely houses Personal Information in its custody as a Research Data Centre under PHIPAA and is responsible for the administration of NB-IRDT.

3.8 *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.

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

3.10 *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 and 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).

3.11 *Personal Information*: As defined in 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.

3.12 *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.

3.13 *Secure Research Environment (SRE)*: 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.

4. POLICY STATEMENTS

4.1 NB-IRDT does not accept Data Sets transferred to the platform that contain direct identifiers, such as name, address (excluding postal code), or unscrambled health card or provider numbers.

4.2 Data must only be used for the purposes for which they were originally approved and must not be otherwise used, shared, or disclosed.

4.3 All NB-IRDT Employees and Approved Data Users are required to provide an appropriate Criminal Record Check, sign a Confidentiality Agreement acknowledging familiarity with NB-IRDT policies, and complete NB-IRDT Data Privacy Training, as well as Security and Orientation Training, prior to accessing data.

4.4 All NB-IRDT Employees and Approved Data Users must participate in NB-IRDT Data Privacy Training once per year.

4.5 Project Principal Investigators must provide NB-IRDT with a recent Curriculum Vitae and the names of all individuals who will have access to the data, as well as their role in the project. Principal Investigators will also be required to sign a Data Access Agreement with NB-IRDT.

5. PROCEDURES

5.1 Security Measures upon Receipt of Data

5.1.1 Master Data Sets are provided by Data Business Owners/Custodians using encrypted media devices (e.g., CD, USB, etc.) which are hand-delivered to the NB-IRDT Database Administrator in the Secure Research Environment at the Fredericton location.

5.1.2 Only the NB-IRDT Database Administrator has regular access to the Master Data Sets and Prepared Data.

5.1.3 An NB-IRDT Senior Data Analyst may be assigned limited access to the Master Data Sets for receipt of data during the absence of the NB-IRDT Database Administrator.

5.1.4 Data must be received in an encrypted form and a login and Password authentication process is used to decrypt the contents of the media devices.

5.1.5 Prior to Data Transfer to the server, media devices are checked to ensure that the data does not include direct identifiers.

5.1.6 The servers that house the data, located in Fredericton and serving all three NB-IRDT sites, are encrypted using whole disk encryption and are Password protected. The servers are locked in a steel cage in an office accessible only by the NB-IRDT Database Administrator and, as necessary, the NB-IRDT Systems Administrator.

5.1.7 Once data are copied from the media devices and placed on the servers, the media devices are stored in a locked safe in the NB-IRDT Database Administrator's office that requires both a physical key and Password for access. The NB-IRDT Senior Data Analyst holds the physical key, and the Systems Administrator holds the Password; neither Employee has access to the other's admission device, and both individuals must be present for the safe to be opened. Each position has an appointed delegate in case of absence.

5.18 A Data Sharing Agreement between the University of New Brunswick (UNB) and the Data Business Owner or Custodian must be signed prior to data being provided for the purpose of matching with data external to NB-IRDT holdings.

5.1.9 External data provided to NB-IRDT by Approved Data Users for Data Matching purposes must have individual identifiers removed by employing the same process used by Data Business Owners/Custodian to prepare Data Sets for transfer to NB-IRDT. The data must be transported to NB-IRDT on a device that has used an encryption algorithm at industry standard.

5.1.10 All syntax programming codes and Approved Data User requests to have codes uploaded into a specific project folder are reviewed by the NB-IRDT Database Administrator prior to upload to ensure the file does not contain any embedded Personal Information.

5.1.11 All syntax programming codes and Approved Data User requests to have codes released (or to re-use in another project) are reviewed by the NB-IRDT Database Administrator prior to being issued to ensure the file does not contain any embedded Personal Information.

5.1.12 Data received for information management purposes are only to be used for the information management purposes and are stored on a separate partition on the server (i.e., not part of the Data Platform) to prevent inadvertent usage for research purposes.

5.2 Workstation Security

5.2.1 NB-IRDT workstations used by Employees and Approved Data Users have been designed to prevent local storage, copying, saving, downloading, or emailing of data.

- Workstations have no output devices that allow for the creation of compact discs, digital tapes, or other comparable media.
- All USB ports are deactivated except for the ports used to connect the workstation mouse and keyboard; no other devices will work in these ports.
- Researcher workstations are not connected to a printer. All printing in the Fredericton location is done on the network printer under the control of the NB-IRDT Database Administrator. On the Saint John and Moncton locations, printing is under the control of the NB-IRDT Satellite Site Employee.
- The network in the NB-IRDT Secure Research Environment has no internet/data connection with any other network or service outside the physical walls of the Secure Research Environment.
- Workstations automatically lock after five (5) minutes of inactivity.
- Approved Data Users can only access their project-specific folders, which contain Data Sets and variables that were approved and for which Data Sharing Agreements were signed.
- The program 'Deep Freeze' automatically runs on all workstations to ensure there are no saved data files on any of the workstations' hard drives. 'Deep Freeze' restores the System to its original state each time it reboots.

5.3 Note Taking Inside the Secure Research Environment

5.3.1 Approved Data Users who wish to make notes while in a NB-IRDT secure facility must use the blue paper provided by the NB-IRDT Database Administrator in Fredericton and the NB-IRDT Satellite Site Employee in Saint John and Moncton. Blue paper is for in-facility use only and does not leave the facility.

5.3.2 Exceptions to release notes on blue paper must be vetted by the NB-IRDT Database Administrator, regardless of site location. A request can be made in person in Fredericton, or by electronic request in project folders for Fredericton and the Satellite Sites. If approved, a copy is made and initialed by the NB-IRDT Administrator for proof of review and made available to the researcher. The original blue paper is securely shredded.

5.3.3 Mobile devices are not permitted for use in the NB-IRDT Secure Research Environment as outlined in the *NB-IRDT Mobile Device Policy*.

5.4 Data Curation Work

5.4.1 NB-IRDT Employees assigned to work on Data Curation for a Data Set, or in relation to a specific project, must submit a *Data Quality Access Request* form to the NB-IRDT Director with carbon copies (cc) submitted to the Database Administrator and Privacy Officer. The request form must clearly state the Data Set being requested for curation as well as the rationale for requiring access to the specific Data Set(s).

5.4.2 If the NB-IRDT Director feels access is warranted for Data Curation work, they will sign the request and send it to the NB-IRDT Employee, with carbon copies (cc) to the NB-IRDT Database Administrator and Privacy Officer.

5.4.3 All data access for Data Curation work must be in keeping with procedures as found in the *NB-IRDT User Access Account Policy*.

6. ADMINISTRATION

6.1 Accountability

6.1.1 The NB-IRDT Database Administrator holds primary responsibility for the security of data during the Data Lifecycle and is responsible for immediately reporting any IT concerns to the NB-IRDT Systems Administrator and any possible Privacy Breaches and/or security breaches to the NB-IRDT Director and NB-IRDT Privacy Officer.

6.1.2 All NB-IRDT Employees are responsible for the general security of data during its access and use at all NB-IRDT Secure Research Environments (i.e., the Hub and Satellite Sites), while ensuring compliance and following NB-IRDT policies. NB-IRDT Employees are to immediately report any IT concerns to the NB-IRDT Systems Administrator as well as any possible Privacy Breaches and/or security breaches to the NB-IRDT Director and NB-IRDT Privacy Officer.

6.1.3 Approved Data Users are responsible to adhere to the privacy requirements and not attempt to circumvent any of the workstation security measures. Approved Data Users are to immediately report any IT concerns to the NB-IRDT Systems Administrator as well as any possible Privacy Breaches and/or security breaches to the NB-IRDT Director and NB-IRDT Privacy Officer.

6.1.4 The NB-IRDT Research & Evaluation Manager, Privacy Officer, and

Database Administrator are responsible to ensure that Approved Data Users have completed all necessary data access requirements as set out in the policies and procedures of NB-IRDT.

6.2 **Monitoring, Auditing, and Reporting**

6.2.1 The NB-IRDT Database Administrator and NB-IRDT Systems Administrator regularly monitor NB-IRDT's Systems to ensure the security of data.

6.2.2 The following table outlines requirements for monthly reports and the NB-IRDT Employee responsible for developing those documents:

NB-IRDT Employee	Report(s)
Database Administrator	• Receipt of Data Sets: i. Date and time of receipt; ii. Who delivered the Data Sets; and iii. The type of data included in the set. • Return of any Data Sets containing direct identifiers • Receipt of External Data Sets for matching purposes • Transfers of data for retention and storage in keeping with the NB-IRDT *Record, Retention, and Destruction Schedule*
Systems Administrator	• Usage logs – list of individuals who accessed specific project folders • Usage log of Database Administrator activities
Data Transfer Coordinator	• Data Transfer Schedule – receipt, returns, destruction, etc., of Data Sets received and securely stored at NB-IRDT
Director Environmental Health, Safety, and Security Department, UNB Saint John	• Secure Research Environment Door Reports – NB-IRDT Saint John
Directeur Service de Sécurité, Université de Moncton, Campus de Moncton	• Secure Research Environment Door Reports – NB-IRDT Moncton
Data Access Coordinator	• Secure Research Environment Door Reports – NB-IRDT Fredericton • Data usage reports reconciled with Approved Data Users and approved data project access
Privacy Officer	• Review, compile, and prepare Audits based on generated reports

6.2.3 The NB-IRDT Privacy Officer compiles reports and submits a summary on request, as well as detailed reports annually to the NB-IRDT Director, Data Business Owners, and Custodians.

7. RELATED DOCUMENTS

- *NB-IRDT Data Access Agreement*
- *NB-IRDT Data Quality Access Request Form*
- *NB-IRDT Data Service Lines of Business*
- *NB-IRDT Dissemination of Research Findings Policy*
- *NB-IRDT Glossary of Data Privacy and Security Terms*
- *NB-IRDT Mobile Device Policy*
- *NB-IRDT Record Retention and Destruction Schedule*
- *NB-IRDT User Access Account Policy*

8. REFERENCES

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

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 for 2018 Expansion	February 2019

Version	**Author**	**Nature of Change**	**Date**
2.1	NB-IRDT Staff	Major Revisions for 2018 Expansion	February 2022

Version	Author	Nature of Change		Date
2.2	NB-IRDT Staff	Content review – slight grammatical & spacing change		June 30, 2022
2.2.1	NB-IRDT Staff	Content review – document titles updating, grammatical & spacing change		May 26, 2023
Approved by VP Research UNB		**Approval Date**	**Effective Date**	**Review Date**
David MaGee		**July 2023**	**July 2023**	**July 2024**