Privacy Breach Policy

1. PURPOSE

1.1 This Policy is a guide for New Brunswick Institute for Research, Data and Training (NB-IRDT) Employees and Approved Users on how to proceed in the event of a Privacy Breach, and to demonstrate to stakeholders that a systematic procedure is in place to respond and deal with such Breaches.

1.2 Activity is considered to be unauthorized if it occurs in contravention of applicable privacy legislation (*Right to Information and Protection of Privacy Act, SNB 2009, c R-10.6 (RTIPPA)* and *Personal Health Information Privacy and Access Act, SNB 2009, c P-7.05 (PHIPAA))*, NB-IRDT policies and procedures, and/or contractual agreements with Government of New Brunswick, Data Business Owners, or Custodians.

1.3 Privacy Breaches also include publishing data and analysis that could lead to the identification (either alone or with other information) of subject individuals, publishing Cells Size Smaller than 5, or removing data outside the secure NB-IRDT environment contrary to data sharing agreements.

2. SCOPE

2.1 This Policy applies to all data-related inquiries, all NB-IRDT Employees and Approved Users, all members serving on NB-IRDT committees, senior University Administration, and Government of New Brunswick Employees serving in advisory capacities to NB-IRDT (e.g. Vice President (Research), University of New Brunswick (UNB), NB-IRDT Advisory Board, Executive Committee, etc.).

3. DEFINITIONS

3.1 *Approved 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 *Cells size smaller than 5:* In research, refers to the number of individuals determined to be exhibiting a specific trait or characteristic being less than 5 individuals (but is not 0).

3.3 *Data Business Owner:* The entity holding legal rights and control over a data set and its variables.

3.4 *Employee(s) (of NB-IRDT):* All full-time and part-time, permanent and contract persons currently earning wages or salary from NB-IRDT (including the Director).

3.5 *New Brunswick Institute for Research, Data and Training (NB-IRDT):* A Research Data Centre as defined in New Brunswick legislation with 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 is composed of three locations, with the Hub located in Fredericton, and Satellite Sites located in Saint John and Moncton. These secure 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 333); and, on the Université de Moncton campus (Bibliothèque Champlain, 415 avenue de l'Université; salle 031).

3.6 *Privacy Audit:* A systematic review and evaluation of privacy practices to measure ongoing compliance with privacy best practices and applicable provincial and federal privacy legislation. It includes following privacy practices through the data life cycle (identification, compilation, access, disclosure and final disposition of data) to identify gaps or potential gaps in data handling practices that may lead to a privacy Breach.

3.7 *Privacy Breach (Breach)*: Occurs when there is an unauthorized collection, use, disclosure, retention, or destruction of personal information as described in Section 49(c) of the Personal Health Information Privacy and Access Act (PHIPAA), including personal health information that has been stolen, lost, or disposed of, except as permitted by the Act. Such activity is unauthorized if it occurs in contravention of applicable privacy legislation (Personal Health Information Privacy and Access Act and Right to Information and Protection of Privacy Act (RTIPPA)) or other applicable legislation.

3.8 *Privacy Breach/Incident Report*: A report resulting from the completion of the Record of Breach – Information on Discovery Form.

3.9 *Privacy Incident:* A situation where a potential for a Privacy Breach existed but was addressed before a Breach occurred.

3.10 Suspected Breach(s): An unconfirmed or perceived occurrence of an unauthorized collection, use, disclosure, retention, or destruction of personal information as described in Section 49(c) of the Personal Health Information Privacy and Access Act (PHIPAA).

4. POLICY STATEMENTS

4.1 NB-IRDT is committed to protecting the privacy, confidentiality, and security of the Personal Information and Personal Health Information located in its databases, and has policies and procedures designed to prevent a Privacy Breach. All NB-IRDT Employees and Approved Users will receive privacy and confidentiality training, which includes the process for handling a suspected or confirmed Breach.

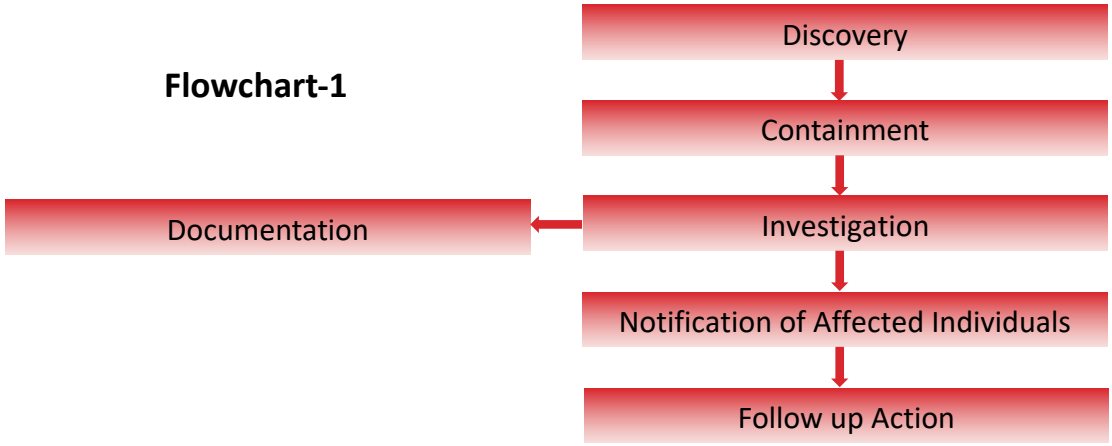
4.2 Upon the discovery of a Personal Information Breach, the NB-IRDT Privacy Officer will, at the first reasonable opportunity when required by law, notify the New Brunswick Integrity Commissioner (“Commissioner”).

4.3 The protocol described below provides a systematic approach for managing a Breach including notification, containment, documentation, investigation, additional notification, and follow up mitigating measures.

5. PROCEDURES

The general order of events that occur upon discovery of a Privacy Breach or Suspected Breach are identified in Flowchart 1; however, it is acknowledged that logistics may require some tasks be completed simultaneously or in a different order.

Flowchart-1



5.1 The following five steps are followed upon discovery of a Privacy Breach or a Suspected Breach or Incident:

Step 1: On Discovery of the Breach

5.1.1 The person who discovers the Breach or Incident will immediately notify the NB-IRDT Director, Privacy Officer, and Senior Data Analyst, or their designates.

5.1.2 The discoverer will document the following information:

- Project title and number (if relevant);
- Date and time of discovery;
- Individuals involved (if known);
- Estimated date and time the Privacy Breach/Incident occurred (if possible);
- Type of Privacy Breach/Incident (e.g., unsecured password, loss, theft, inadvertent disclosure, maintenance of data past destruction, etc.). The discoverer describes the situation, but does not make the determination whether the situation constitutes a Breach or an Incident; and,
- Type of data involved (e.g., included direct personal identifiers, encrypted data, etc.).

5.1.3 The NB-IRDT Privacy Officer will notify the University Secretary, Records Management, Access and Privacy Coordinator ("UNB Privacy Coordinator"), and

the applicable Data Business Owner(s)/Custodian(s).

5.1.4 In the event of a Personal Health Information Breach the Privacy Officer will notify the Commissioner and provide the following information:

- The individual's contact information;
- A description of the nature of the Breach;
- The date and location of the Breach; and,
- The date the Breach came to the attention of the NB-IRDT Privacy Officer.

Step 2: Containment

5.1.5 The process of containment is to be initiated as soon as possible to prevent release or further release of Personal Information or Personal Health Information. Steps toward containment are taken by the first person who becomes aware of the or Incident and has the ability and authority to do so. Some of these steps can be taken by the discoverer and/or NB-IRDT Privacy Officer, whereas other steps require intervention by the NB-IRDT Senior Data Analyst, the Director, and/or the Systems Administrator.

5.1.6 The containment processes include:

- Determine what, if any, information has been disclosed;
- Retrieve as much of the Breached information as possible (ideally all Breached information);
- Ensure no copies of Personal Information or Personal Health Information have been made or retained by the unauthorized person(s);
- Ensure that additional Breaches cannot occur through the same means;
- Determine whether the Privacy Breach would allow unauthorized access to any other Personal Information or Personal Health Information (e.g. an electronic information system) and take whatever necessary steps to contain the situation (e.g. change passwords, identification numbers, and/or temporarily shut down a system); and,
- Document all above information and be prepared to review with the NB-IRDT Privacy Officer.

5.1.7 The following steps are intended to illustrate the actions that may be required to contain the Privacy Breach, Suspected Breach, or Incident – but are not exhaustive. Individual circumstances will dictate particular requirements.

- If an electronic data device is stolen from NB-IRDT, notify security and the police immediately to determine if the person who removed the device is still in the building or vicinity;

- Confirmation of email addresses will be made before sending any Personal Information;
- If an email was sent to the wrong person, call the recipient and ask them to securely destroy any email printouts that were made, delete the email, and confirm in writing that the document was securely destroyed, no copies were made or kept, and that information will not be shared in any circumstances;
- If an unauthorized person has or may have access to a database notify the NB-IRDT Senior Data Analyst, who will disable accounts or change passwords and identification numbers; and,
- Where unauthorized verbal disclosure has occurred, request that the recipient of the personal or sensitive Information treat it confidentially.

Step 3: Investigation and Documentation

5.1.8 The NB-IRDT Director, Privacy Officer, and Senior Data Analyst will investigate the Breach, initiate procedures, and impose sanctions consistent with relevant UNB policies.

5.1.9 Breach/Incident investigations include the following elements:

- Interviewing individuals involved with the Privacy Breach or Incident, or individuals who can provide information about the process and confirm details on the *Record of Privacy Breach/Incident Form*;
- Ensuring any issues surrounding containment and notification have been addressed by NB-IRDT; and,
- Obtaining any relevant evidence.

5.1.10 The NB-IRDT Privacy Officer (or designate) is responsible for the documentation of the Breach/Incident and will complete the Privacy Breach/Incident Report using a *Record of Privacy Breach/Incident Form*.

Step 4: Notification of Affected Individuals

5.1.11 The NB-IRDT Privacy Officer, in conjunction with the Commissioner (when appropriate), the UNB Privacy Coordinator, and appropriate Data Business Owner(s)/Custodian(s) will determine whether notification to individuals to whom the information relates is possible and/or required. Any notification may be completed jointly with the Data Business Owner(s)/Custodian(s) and/or the UNB Privacy Coordinator.

5.1.12 Exemption to notification regarding Personal Health Information may occur only if none of the following three situations as stated in section 49(2) of PHIPAA will occur as a result of the Breach. Notification is not required if the Breach will not:

- have an adverse impact on the provision of health care or other benefits to the individual to whom the information relates;
- have an adverse impact on the mental, physical, economic, or social well-being of the individual to whom the information relates; and,
- lead to the identification of the individual to whom the information relates.

Step 5: Follow up Action

5.1.13 The Commissioner may investigate notices of Privacy Breach involving NB-IRDT. In such an event, the Privacy Officer will cooperate fully with the Commissioner to:

- Review the steps taken to contain the Breach;
- Ensure the notification of affected individuals (as applicable);
- Review the circumstances surrounding the Breach in an attempt to fully understand the scope and cause of the Breach;
- Determine appropriate corrective mitigating measures to reduce future risk; and,
- Follow and implement recommendations for corrective measures as provided by the Commissioner.

5.1.14 Upon completion of the Investigation, a plan will be developed to identify the root cause(s) of the Breach or Incident and implement corrective and preventative measures (prevention plan). The following list of preventive measures is intended to illustrate the actions that may be taken, but is not an exhaustive list. Individual circumstances will dictate the required actions.

- Determine whether the Privacy Breach protocol was followed;
- Conduct a Privacy Audit of administrative, physical, and technical safeguards, and correct any deficiencies;
- Educate NB-IRDT Employees and Approved Users on how to avoid similar Breaches;
- If the Privacy Breach was due to a discrepancy between Policy and practice, educate all relevant persons to ensure greater awareness of the expected practices (based on the existing policies);
- If the Privacy Breach was due to a weakness in an existing Policy, revise the Policy and notify all relevant persons about the revision; and,
- Review the privacy and security training program to identify and rectify gaps.

5.1.15 Where an NB-IRDT Employee caused the Breach, the applicable UNB Employee Agreement will be consulted regarding discipline and appropriate sanctions made.

5.1.16 In the situation where a non-Employee of NB-IRDT was the cause of the Privacy Incident/Breach, the NB-IRDT Director will inform the individual's employer or faculty advisor (if a student) of the circumstances of the Breach in writing within 24 hours.

5.1.17 NB-IRDT reserves the right to disallow access to NB-IRDT data for persons who have been the cause of a Privacy Breach.

6. ADMINISTRATION

6.1 Accountability

6.1.1 All NB-IRDT Employees and Approved Users are responsible to immediately report a suspected or confirmed Breach of privacy/security to the appropriate person and follow the protocol as the discoverer of the Breach.

6.1.2 The NB-IRDT Employee, Director, Privacy Officer, and/or Senior Data Analyst is responsible to ensure proper containment of the Breach; provide appropriate notification; document and report the Breach; take action to prevent future Breaches; and, follow up with monitoring and Privacy Audits as listed in Section 7 of this Policy.

6.1.3 The Privacy Officer is responsible to report the Breach to the Data Business Owner(s)/Custodian(s) and the Commissioner under PHIPAA, ensure all appropriate documentation is completed and signed, assist with the investigation as required, notify others as required, conduct the review, and develop and/or implement the remedial plan.

6.1.4 The Privacy Officer is responsible to ensure the completion of the Privacy Breach/Incident Report in full using a *Record of Privacy Breach/Incident Form*.

6.1.5 The NB-IRDT Director is responsible to notify the relevant employer/faculty advisor and follow the appropriate UNB processes and provincial legislation penalties.

6.2 Monitoring, Auditing and Reporting

6.2.1 Following any Privacy Breach investigation, the NB-IRDT Director and Privacy Officer will review this Policy to determine its effectiveness and revise accordingly.

6.2.2 The NB-IRDT Privacy Officer, Senior Data Analyst, and/or Systems Administrator will conduct a Privacy Audit following a privacy/security Breach to ensure that any planned changes to procedures/processes have been implemented.

6.2.3 Privacy Breach Reports are submitted by the NB-IRDT Privacy Officer to the NB-IRDT Director and the Executive Director of the Office of Research Services at UNB annually, or on request. Reports must detail any privacy and/or security Breaches or Incidents, describe investigation and mitigating measures, as well as proposed actions for preventing similar Breaches or Incidents in the future.

6.2.4 In accordance with the Originating Agreement and the Operating Agreement with the Government of New Brunswick, and any master data sharing agreements with Data Business Owners/Custodians, the NB-IRDT Director will provide each Data Business Owner/Custodian with an annual report detailing the following:

- A list of all persons who were approved to access NB-IRDT data along with the purpose for the access;
- A summary of the risks identified through current Privacy Impact Assessment and Threat and Risk Assessment; and,
- A summary of any changes to its operating procedures, governance structure, privacy, or security policies or protocols.

Copies of the summary of risk identified through the aforementioned assessments and any changes to operating procedures, governance structure, privacy or security policies, or protocols of NB-IRDT will be provided to the Office of the Integrity Commissioner for New Brunswick.

7. DOCUMENTS

- *NB-IRDT Record of Breach/Incident – Information on Discovery Form*
- *NB-IRDT Glossary of Terms and Acronyms*

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		March 2017
Approved by		**Approval Date**	**Effective Date**	**Review Date**
Vice President (Research)		March 2017	March 2017	September 2017

Version	**Author**	**Nature of Change**		**Date**
1.1	D. Curtis Maillet	Minor Revisions for 2018 Expansion		July 2018
Approved by		**Approval Date**	**Effective Date**	**Review Date**
				September 2019

Version	Author	Nature of Change		Date
1.2	D. Curtis Maillet	Minor Revisions, definitions updated		July 2018
Approved by		**Approval Date**	**Effective Date**	**Review Date**
Vice President (Research)		November 2019	November 2019	July 2020