Lakehead University

Research Data Guidelines and Classification Standard

This Guidelines and Standard document is intended for the use of Lakehead University.

Record of Changes

Change No.	Date	Change Detail	Approved By (Name):
		Initial Release	

Table of Contents

1.0 Purpose

The purpose of this document is to outline the guidelines and standard for the classification, management, and protection of research data at Lakehead University (the University) to ensure the quality, integrity, security, and authorized accessibility of research data. These guidelines establish defined roles and responsibilities for the management of the University's research data, incorporates regulatory requirements and industry practices, and outlines the organizational guidelines to standardize the management and governance of research data at the University. The guidelines help ensure that the University's research data is managed and safeguarded in alignment with the Government of Canada's Tri-Agency Research Data Management Policy and the Safeguarding Your Research Guidelines.

2.0 Scope

This guidelines and standard document applies to the Office of Research Services, all University researchers (Principal Investigator and research team members), Technology Services department (IT), and any third parties who support researchers' activities and/or are authorized to access the University's research data. These guidelines apply to **research data that is within the researcher's control** and is within the University's environment (data hosted within on-premise and cloud systems) including any research data **stored on University-provided systems / devices**.

These guidelines do not apply to data used in research that is stored by a third party outside of the control of the University that researchers are provided access to (e.g., research participants' data that is collected by a hospital or community partner and stored and managed within their respective databases before being provided to the University's researchers).

These guidelines apply to **all research activities at the University**, regardless of whether or not it is Tri-agency funded research.

All research data, regardless of format such as on paper (e.g., written notes, printed files) or electronic such as database records, video and audio recordings, and data files (e.g., Word documents, Excel spreadsheets) stored on University-provided devices/systems, are covered by this guidelines and standard document, unless specifically exempted by the **Director, Office of Research Services**.

Research Involving Indigenous Peoples in Canada

For research involving Indigenous peoples in Canada, ownership of research data is governed by the First Nations Principles of OCAP®. While Lakehead's Research Data Classification Guidelines broadly apply to the University's research data, these guidelines do not supersede the Principles of OCAP® when research data involves First Nations, Inuit, or Métis participants.

Where divergences exist between the application of OCAP® and Lakehead's Research Data Classification Guidelines, they should be addressed and resolved in consultation with the Office of Research Services prior to the commencement of a research project.

3.0 Audience

The audience of these guidelines are those who are responsible for collecting, classifying, managing, protecting, using, and sharing research data at the University.

4.0 Data Governance

4.1 Data Governance Roles and Responsibilities

This section describes the role definitions and associated responsibilities for the proper governance and management of research data throughout the information lifecycle.

4.1.1 Director, Office of Research Services Responsibilities

The **Director, Office of Research Services** oversees and manages the central office providing research administrative services to the research community at the University and ensures that policies and procedures to manage and safeguard research data are developed, maintained, and implemented across the University. The responsibilities of this role are as follows:

- Develop and maintain the Research Data Guidelines and Classification Standard.
- Oversee and monitor the University's adherence to these guidelines.
- Maintain a data sharing agreement template for researchers that can be used when research data is shared with third parties.
- Maintain a research agreement template for researchers that can be used when research involves Indigenous peoples and Indigenous data
- Monitor and communicate changes to researchers on privacy legislation that will impact the management of research data.

4.1.2 Principal Investigator Responsibilities

A **Principal Investigator** is an individual at the University ultimately responsible for a research project and accountable for the proper management and safeguarding of research data under their control and that is within the University's environment. For research involving Indigenous peoples in Canada, ownership of research data is governed by the First Nations Principles of OCAP®. The Principal Investigator's responsibilities are as follows:

- Understand the standard referenced by this document and handle all research data in accordance with the guidelines and standard.
- Understand the data that is being created, collected, and used for their research activities and how it flows throughout the information lifecycle by developing and maintaining a personal information inventory (PII inventory).
    - The PII inventory should detail the data elements collected for research activities and how they flow throughout the information lifecycle (collection, processing/analysis, storage, safeguarding, sharing, dissemination of research findings, destruction). The inventory should be **reviewed on a periodic basis** (e.g., quarterly) to ensure accuracy and updated accordingly, or as there are any changes in the process(es) that involve the collection or processing of personal information.
- Assign an appropriate sensitivity level to research data based on the ***Data Classification Levels*** as outlined in **Section *5.1.***
- Identify the appropriate handling standard associated with the assigned sensitivity level as described in ***Section 5.0 – Data Classification Standard***.
- Implement (and/or delegate responsibilities for implementing) appropriate data handling standard to research team members and IT.
- Ensure all research team members being onboarded for a project receive training on the data handling standard outlined in this document.

4.1.3 Research Team Member Responsibilities

A **Research Team Member** is an individual at the University recruited to support the Principal Investigator in their research activities. This could refer to an undergraduate or graduate student, a post-doctoral fellow, another researcher working under the supervision of the Principal Investigator, or personnel externally hired and working under the direction of the Principal Investigator. The Research Team Member's responsibilities are as follows:

- Understand the standard referenced by this document and handle all research data in accordance with the guidelines and standard.
- Implement the appropriate data handling standard for the various sensitivity levels as identified by the Principal Investigator.
- Collaborate with IT for support in implementing the technical controls within systems / applications that are used for research activities in alignment with data handling guidelines.

4.1.4 IT Responsibilities

IT, under the leadership and direction of the **Director, Technology Services**, oversees and manages the University's technology infrastructure and provides support to the Office of Research Services in developing and implementing policies and procedures to manage and safeguard research data within the University's environment, including any research data stored on University-provided systems / devices. IT's responsibilities are as follows:

- Understand the standard referenced by this document and handle all research data in accordance with the guidelines and standard.
- Implement the appropriate data handling standard for the various sensitivity levels as identified by the Principal Investigator.
- Provide support to Principal Investigators and research team members in implementing the technical controls within systems / applications that are used for research activities in alignment with data handling standard.
- Provide support to Principal Investigators and research team members with approved technological solutions that meet the data handling standard outlined in this policy based on sensitivity.

4.2 Data Handling Guidelines

4.2.1 – All research data should be managed in accordance with their value, sensitivity, and risk levels.

4.2.2 – The collection and use of research data containing human participants' personal information should be limited only to what is necessary for answering the research question(s).

4.2.3 – All research data should be retained in accordance with the applicable retention schedule and requirements (as defined by the LUFA Collective Agreement or by another contractual agreement that the data is subject to) and securely disposed of (through archival or destruction) once the retention period has elapsed.

4.2.4 – Any **Confidential** research data (as defined by the section *Data Classification Scheme*) that is being shared with third parties should have a data sharing agreement in place to ensure that the information shared will be adequately safeguarded by the third party as per the University's requirements. The controls defined within any data sharing agreements with third parties should align with the guidelines outlined in this document.

4.2.5 – The handling and treatment of data should be implemented in a way that when combined with effective security controls, ensures the data is safeguarded from unauthorized access, manipulation, or inadvertent disclosure.

4.2.6 – All research data should be reviewed to determine a classification level; a single classification level should be assigned to a collection of data that is common in purpose or function.

4.2.7 – All research data should be handled in a manner that is in line with its classification level as laid out in the section *Data Classification Standard*.

5.0 Data Classification Standard

5.1 Data Classification Levels

Data classification, in the context of information security, is the classification of data based on its level of sensitivity and the impact to the University should that data be disclosed, altered, or destroyed without authorization. The classification of data helps determine what baseline security controls are appropriate for safeguarding that data.

Three classification levels have been outlined below along with a brief description and examples of data elements mapped to each classification level.

All research data should be evaluated, classified, and safeguarded in accordance with its sensitivity level. Assignment of sensitivity level is to be based on a consideration of the legal obligations to protect the confidentiality of the information, as well as the **risk of harm that may result** from the information's unauthorized access, manipulation, or inadvertent disclosure.

In alignment with TCPS 2 (2022), assessment of risk level should consider the **magnitude or seriousness of the harm** and the **probability that this harm will occur** to research participants and/or the University should the research data be subject to unauthorized access, manipulation, or inadvertent disclosure.

Harm is anything that has a negative effect on the welfare of participants and/or the University, and the nature of the harm may be social, behavioral, psychological, physical, or economic.

When assessing risk associated with research data, consider that the aggregation of different risk factors can increase the overall risk level.

All research data should be classified into one of three classification levels as shown in the table below:

	Classification Levels		
	Confidential / Sensitive	**Internal / Private**	**Public**
Definition	Research data only available to limited authorized individuals; unauthorized disclosure could result in severe harm to an individual or the University.	Research data available to authorized users for research purposes; unauthorized disclosure could result in minor harm to an individual or the University.	Research data that is deemed public by legislation or through a University policy; disclosure would not result in any harm to an individual or the University.
Risk	There is a **notable to significant risk** of unauthorized disclosure resulting in: ▪ Diminished trust and confidence in research data and results ▪ Loss of research data ▪ Loss of exclusive control over intellectual property, patent opportunities, and potential revenue ▪ Legal or administrative consequences ▪ Loss of potential future partnerships ▪ Tarnished reputation	There is a **minor risk** of unauthorized disclosure resulting in: ▪ Diminished trust and confidence in research data and results ▪ Loss of research data ▪ Loss of exclusive control over intellectual property, patent opportunities, and potential revenue ▪ Legal or administrative consequences ▪ Loss of potential future partnerships ▪ Tarnished reputation	Disclosure **will not result in any harm or injury** to an individual or the University and does not require prior authorization.

Examples of Data Elements	▪ Human participants' personally identifiable information (PII) such as:
	  ○ Name
	  ○ Date of Birth
	  ○ Address
	▪ Human participants' sensitive personal information such as:
	  ○ Sexual orientation
	  ○ personal health and medical information (e.g., health diagnosis)
	  ○ financial information (e.g., income)
	▪ De-identified human participants' data (where the risk of re-identification remains)
	▪ Intellectual property
	▪ Unpublished research data, library transactions and journals
		▪ Internal meeting minutes / notes / correspondence shared among the research team
		▪ Contracts between researchers and other parties (e.g., other institutions, community partners, industry partners)
		▪ Research project funders or prospective funders name and contact information
			▪ Published research data
			▪ Public announcements
			▪ News articles
			▪ Annual reports
			▪ Names of researchers and their business contact information
			▪ Aggregated human subject data (where re-identification is not possible) where research participants are aware that their anonymized data will be made public through dissemination.

5.2 Data Classification and Controls Standard

The objective of the data classification and controls standard is to provide researchers with an easy-to-understand document that allows them to determine how research data should be safeguarded based on the classification at each stage of their information lifecycle.

Data Controls Standard Exceptions

In cases of exception where the data controls standard is not able to be adhered to due to system or business limitations, a compensating control should be identified and implemented to meet the objectives of the original intent of the standard and mitigate the risk of unauthorized disclosure. **Any case of exception to the standard should be documented and communicated in writing to the Office of Research Services.**

	Data Classification Scheme – *Controls Standard*		
	Confidential / Sensitive	**Internal / Private**	**Public**
Consent and Secondary Use of Research Data	**Voluntary and informed consent** must be obtained from research participants (or an appropriate proxy) before or at the time of the collection, which includes consent to the use of the data collected for specific purposes. Consent to participate in research should be obtained even if data contains no personally identifiable information (PII). Researchers should **be aware of the first language of Indigenous participants**, and if it is an Indigenous language, researchers should **make available translation** by a knowledgeable person during the consent process. For **secondary use** of data containing identifiable information, **express and informed consent must be obtained** before use unless the researcher can satisfy the terms of TCPS Article 5.5A For secondary use of anonymous data, researchers are not required to seek consent.	No specific standard	No specific standard
Data Disclosure / Sharing	No **Confidential** research data shall be **disclosed** to other research teams or departments at the University, or to 3rd parties, without the **Principal Investigator** and the **research participant's express and informed consent.** **Purpose(s) for the disclosure** of research participants' personal information **should be**	**Third parties' access to Internal research data should have in place**: ▪ Review and approval from the Principal Investigator, and, if human participant data, express and informed consent from the research participants.	No specific standard

	Data Classification Scheme – *Controls Standard*		
	Confidential / Sensitive	**Internal / Private**	**Public**
	limited to what was identified at the time of their consent being obtained. **Third parties' access to data should have in place**: ▪ Data sharing agreement that documents controls aligned with document ▪ NDA ▪ Review and approval from the Principal Investigator.		
Access Provisioning	**Access** should be provisioned **based on roles** on the research team and on a need-to-know basis **Authorization should be obtained** to view or edit data; access should be based on **least privilege access principle**. Any exceptions for granting access should be obtained from the Principal Investigator. For research team members accessing data via remote-access technologies, **prohibit copying, moving,** and **downloading** research data onto local drives and removable media (e.g., USB), unless explicitly authorized by the Principal Investigator for a defined purpose.	Grant access to research team members as needed. **Access** should be **authorized** and **approved** by the Principal Investigator.	No specific standard
Access Monitoring	Review the list of team members who have access to **Confidential** research data on a **regular** basis (e.g., quarterly) to **identify** where **access is no longer required** for certain individuals.	Review the list of team members who have access to **Internal** research data on a **regular** basis (e.g., quarterly) to identify where access is no longer required for certain individuals.	No specific standard

	Data Classification Scheme – *Controls Standard*		
	Confidential / Sensitive	**Internal / Private**	**Public**
	Access to data should be **reviewed for all systems** and applications that are identified in the Principal Investigator's personal information inventory.		
Access De-provisioning	Based on regular review of the list of team members who have access to **Confidential** research data, revoke access for individuals who no longer require access. Immediately **revoke access for terminated** research team members. **Remove/disable inactive user accounts within 90 days** unless otherwise specified or approved by the Principal Investigator.	Based on regular review of the list of team members who have access to **Internal research d**ata, revoke access for individuals who no longer require access. **Remove/disable inactive user accounts within 90 days** unless otherwise specified or approved.	No specific standard
Electronic Storage	**Restrict** the electronic **storage** of **Confidential** research data to **University-provided** desktop/laptop, databases, and authorized SaaS applications. In **cases of exception** where removal media is used to store data, **engage IT** to ensure that it **is encrypted**, and **password protected** prior to usage. **Archived Data:** Data should be **encrypted** when **archived** and **RBAC** (role-based access control) mechanisms should be leveraged.	Store **Internal** research data on University-provided desktop/laptop, databases, and authorized SaaS applications. **Archived Data:** No specific standard **Cloud:** No specific standard **Databases / Shared Drives / Laptops / Workstations:** No specific standard	No specific standard

	Data Classification Scheme – *Controls Standard*		
	Confidential / Sensitive	**Internal / Private**	**Public**
Physical Storage	Hardcopy (paper-based) **Confidential** research data should always be **stored in a locked container** (e.g., filing cabinet) with the key accessible only by the Principal Investigator unless otherwise approved and authorized. Data **should not be left in plain view** unattended.	Use reasonable precautions to **restrict display** and **access** to **Internal** research data.	No specific standard
Backups	**Backups** of **Confidential** research data to other media for storage should be **encrypted** and **password protected** to protect against accidental or intentional disclosure. Backups of hardcopy (paper-based) data should be **stored in a locked container** (e.g., filing cabinet).	No specific standard	No specific standard
Electronic Transmission	**Emails:** **Confidential** research data should not be transmitted through email. In cases of exception, emails containing **Confidential** information should: ▪ be encrypted; ▪ include the **Email Notice Disclaimer** outlined below **at the beginning of the email;** and ▪ Include the label **'Confidential'** in the email subject line. **Sharing:** **Sharing of data** is done only via **secure and authorized** means that have been **approved by IT** (e.g., secure file transfer protocol). In **cases of exception** where removal media are used for the sharing of data, engage IT to ensure	**Emails:** ▪ Emails containing **Internal** research data should include the **Email Notice Disclaimer** outlined below **at the beginning of the email** **Sharing:** **Sharing of data** within the University is done via **internal systems** that have been **approved by IT** (e.g., SharePoint, OneDrive). **Distribution** of research data is **restricted to named individual(s)** only.	**Emails:** No specific standard **Sharing:** No specific standard

	Data Classification Scheme – *Controls Standard*		
	Confidential / Sensitive	**Internal / Private**	**Public**
	that it is **encrypted,** and **password protected** prior to usage. **Distribution** of data is **restricted to named individual(s)** only.		
	Email Notice Disclaimer: "Notice: The information contained in this message is proprietary data belonging to Lakehead University and is intended for the confidential use of the addressee. If you are not the addressee, you are hereby notified that you have received this message in error and that any review, dissemination, distribution or copying of this message is strictly prohibited. If you have received this message in error, please notify us immediately."		
Physical Transmission	Ensure **sensitivity level** is always **reproduced** when moving hardcopy (paper-based) **Confidential** research data Use **tamper evident packaging**; label as "**Confidential**"	Use **sealed envelope.**	No specific standard
Data Retention	**All research data, including confidential** research data, is to be retained for a minimum of **7 years after the completion of research activities,** as defined by the LUFA Collective Agreement. If the research data is subject to a separate retention schedule based on specific contractual agreements, **retain the data** based on the **applicable retention schedule.** Data that is **identified** by the Principal Investigator as ready for destruction or archival should also	**Internal** research data is to be retained for a minimum of **7 years after the completion of research activities,** as defined by the LUFA Collective Agreement. If the research data is subject to a separate retention schedule based on specific contractual agreements, **retain the data** based on the **applicable retention schedule.**	No specific standard

	Data Classification Scheme – *Controls Standard*		
	Confidential / Sensitive	**Internal / Private**	**Public**
	identify all the systems / applications where this data exists (as per the PII inventory) to ensure that all applicable data is destroyed or archived. Data that is up for destruction or archival (i.e., the retention period has elapsed) **should be approved** by the Principal Investigator before it is destroyed or archived. **Retaining a Copy of Data Shared with Third Parties:** For compliance purposes, when collaborating with and sharing data with external third parties, **one copy of the data must be retained by the University** for the minimum of 7 years or as otherwise required based on specific contractual agreements.		
Data Disposal & Destruction Methods	**Securely dispose of data through the appropriate means** (destruction or archival) in accordance with the applicable data retention requirements. **Hardcopy (paper-based) Data:** **Shred** and **obtain a certificate of destruction** if it is outsourced to a third party. **Electronic Data:** **Destroy** data, including backups, using a process that ensures the data **cannot be recovered and used** for unauthorized purposes.	**Securely dispose of data through the appropriate means** (destruction or archival) in accordance with the applicable data retention requirements. **Hardcopy (paper-based) Data:** **Shred** or **place in secure recycling container.** **Electronic Data:** Delete. **Physical Devices:** Return University-provided devices to the Facilities team for secure disposal. Engage IT for guidance	**Securely dispose of data through the appropriate means** (destruction or archival) in accordance with the applicable data retention requirements. **Hardcopy (paper-based) Data:** Use any method of destruction. **Electronic Data:** Delete. **Physical Devices:**

	Data Classification Scheme – *Controls Standard*		
	Confidential / Sensitive	**Internal / Private**	**Public**
	Physical Devices: Return University-provided devices to the Facilities team for secure disposal. Engage IT for guidance and support with return of physical devices if needed. All devices or digital storage media should be **destroyed** using a process that absolutely ensures the data on the device or media is **rendered totally and permanently inaccessible.** Obtain a certificate of destruction if it is outsourced to a third party. **Third Parties** Upon termination, cancellation, expiration, or conclusion of a 3rd party contract, the service provider should **return data to the University unless** the University requests that the data be **destroyed by the 3rd party.** Within a thirty (30) day period, the 3rd party service provider should **certify** in writing to the University that such return or **destruction** has been **completed**.	and support with return of physical devices if needed. **Third Parties** N/A	Return University-provided devices to the Facilities team for secure disposal. Engage IT for guidance and support with return of physical devices if needed. **Third Parties** N/A
Training	**Provide training** to research team members handling **Confidential** research data to help them identify and implement the controls outlined in this document.	**Provide training** to research team members handling **Internal** research data to help them identify and implement the controls outlined in this document.	No specific standard

	Data Classification Scheme – *Controls Standard*		
	Confidential / Sensitive	**Internal / Private**	**Public**
Reporting	If **Confidential** research data is inadvertently sent to or received by the wrong recipient, contact the **Office of Research Services** for guidance and, if required, escalate to the **Director of Risk Management and Access to Information and the Director of Technology Services**. Refer to the **Research Integrity Policy and Procedures** for additional guidance on reporting breaches related to the quality, thoroughness, and integrity of research activities.	No specific standard	No specific standard
Audit Logs of Access to Data	**Audit trails should be enabled** for systems/applications that contain **Confidential** research data to track user activities (e.g., access, edits, downloads). **Access** to data should be **approved, authenticated, and logged.** **Review audit logs** to investigate user activities when there is a suspected or reported privacy or security incident. **Retain audit logs** for at least a year with a minimum of two months immediately available for analysis.	**Audit trails should be enabled** for systems/applications that contain **Internal** research data (e.g., access, edits, downloads). **Review audit logs** to investigate user activities when there is a suspected or reported privacy or security incident. **Retain audit logs** for at least a year with a minimum of two months immediately available for analysis.	No audit log review needed No audit log retention needed
Threat and Vulnerability Management	Systems, applications, and servers containing **Confidential** research data should go through **threat and vulnerability management testing** on a monthly basis.	Systems, applications, and servers containing **Internal** research data should go through **threat and vulnerability management testing** on a monthly basis.	No specific standard

	Data Classification Scheme – *Controls Standard*		
	Confidential / Sensitive	**Internal / Private**	**Public**
	Vulnerability scans should be performed monthly. **Rescans (repeated scans) should be performed** after a significant change to the system/application/server, or to test and inspect that a vulnerability identified has been remediated. Notify the University's **Director of Risk Management and Access to Information** and **the Director of Technology Services** as well as the applicable regulators and/or law enforcement of any occurrence or breach of privacy as soon as possible after discovery and provide fixes or upgrades for security vulnerability within 90 days of discovery.		

6.0 Related Policies, Procedures and Guidelines

This guidelines and standard document should be read in conjunction with:

- Tri-Agency Research Data Management Policy
  - Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans – TCPS 2 (2022)
  - Tri-Agency Statement of Principles on Digital Data Management
  - TCPS 2 (2022) – Chapter 9: Research Involving the First Nations, Inuit, and Métis Peoples of Canada
- Safeguarding Your Research Guidelines
- The First Nations Principles of OCAP®
- LUFA Agreement
- IT Security Policy
- Research Integrity Policy and Procedures
- Lakehead Data Sharing Agreement Template

7.0 Definitions

Term	Definition	Examples
Availability	**Availability relates to ensuring timely and reliable access to and use of data.** Availability ensures that authorized users have access to data when required. Availability is the property of data being accessible and usable upon demand by an authorized party. Data security controls ensure that data is available to authorized parties whenever they need to access them.	N/A
Confidentiality	**Confidentiality relates to preserving authorized restrictions on data access and disclosure.** Confidentiality ensures that data can only be accessed by authorized individuals and is not made available or disclosed to unauthorized individuals or entities.	Implementing controls (e.g., Least Privilege Access Principle) to protect data from being viewed and edited from unauthorized parties.
Data Classification	The classification label that is assigned to all research data to help identify the level of sensitivity for that data and the controls that should be implemented to properly handle and protect the data.	▪ Confidential ▪ Internal ▪ Public
De-identification	As defined by Bill C-27, de-identification is the modification of personal information so that an individual cannot be directly identified from it. **Note**: However, a risk of the individual being identified remains.	N/A

Human Participants	As defined by the Tri-Agency Research Data Management Policy, human participants (or research participants) are those individuals whose data, biological materials, or responses to interventions, stimuli, or questions by the researcher, are relevant to answering the research question(s).	▪ University Psychology students ▪ Patients enrolled in a clinical trial ▪ People taking surveys on SurveyMonkey ▪ Police officers ▪ Individuals from vulnerable populations
Information	Recorded information in any form, in any medium, and at all stages of its lifecycle including information created, recorded, transmitted, or stored in digital form or in other intangible forms by electronic, magnetic, optical or any other means, but does not include a mechanism or system for creating, sending, receiving, storing or otherwise processing information.	▪ Research data ▪ Signed participant consent forms ▪ Interview transcripts ▪ Internal policies and procedures
Integrity	**Integrity relates to the rights to change data.** Integrity ensures that only authorized and accurate changes are made to data. Integrity is the property of data accuracy and completeness and refers to the level of protection necessary to prevent data from being modified by unauthorized parties.	N/A
Least Privilege Access Principle	This is an information security principle that refers to a user being given the minimum levels of access or permissions required to perform their job function.	A research assistant being provided access only to folders on the shared drive for the project that they are working on and not any additional access to other project folders.
Lifecycle	The stages that specific data classes, categories or elements go through from creation or capture to destruction.	▪ Create ▪ Store ▪ Use ▪ Share ▪ Archive ▪ Destroy
OCAP® Principles	The First Nations principles of OCAP® establish how First Nations' data and information will be collected, protected, used, or shared. OCAP® asserts that First Nations alone have control over data collection processes in their communities, and that they own and control	OCAP® Principles cover: ▪ Ownership ▪ Control ▪ Access ▪ Possession

	how this information can be stored, interpreted, used, or shared.	
Personal Information	As defined by PIPEDA, personal information refers to any factual or subjective information, recorded or not, about an identifiable individual.	Research participants': ▪ Name ▪ Date of Birth ▪ Gender ▪ Sex ▪ Health Information
Privacy	**Privacy relates to research participants' right to have control over how their personal information is collected, used, and disclosed**. An individual's right to privacy is protected by law. This law informs data classification and the level of protection necessary to prevent access and disclosure of research participants' personal information to unauthorized parties.	N/A
Research Data	As defined by the Tri-Agency Research Data Management Policy, research data are data that are used as primary sources to support technical or scientific enquiry, research, scholarship, or creative practice, and that are used as evidence in the research process and/or are commonly accepted in the research community as necessary to validate research findings and results. Research data may be experimental data, observational data, operational data, third party data, public sector data, monitoring data, processed data, or repurposed data.	▪ De-identified human participants data ▪ Identifiable human participants data ▪ Interview audio recordings
Unauthorized Access	Unauthorized access refers to the collection, use, or disclosure of an individual's personal information without their consent and for purposes that are beyond what is required.	A research team member accessing research participants' personal information for a project that the team member is not assigned to.