



<b>Policy Number:</b>	61
Approval Date:	March 2023
Implementation Date:	March 2023
Approved By:	VP of Operations
Upcoming Review:	March 2028

## **Research Data Management Policy**

### **Purpose**

The purpose of this Research Data Management Policy is to ensure that research data generated or used by the ACATCM is collected, managed, stored, and shared in a way that complies with relevant legislation, including the Personal Information Protection Act (PIPA), the Freedom of Information and Protection of Privacy Act (FOIP), and the Health Information Act (HIA).

### **Scope**

This policy applies to all ACATCM faculty, staff, students, and anyone else involved in conducting research using ACATCM resources or generating research data that will be stored on ACATCM's information systems.

### **Policy Statement**

ACATCM recognizes that research data is a valuable asset that must be managed throughout the research lifecycle. To protect the privacy of research participants and comply with relevant legislation, ACATCM will:

- a. Collect, use, and disclose research data only for the purposes for which it was collected or for a use consistent with that purpose, unless the research participant has provided explicit consent for another use or disclosure;
- b. Implement appropriate physical, technical, and administrative safeguards to protect research data from loss, theft, unauthorized access, use, or disclosure;
- c. Retain research data only for as long as necessary to fulfill the purpose for which it was collected or as required by law, and then securely dispose of it;
- d. Ensure that research data is shared only with authorized personnel or entities for the purposes of the research, and only to the extent necessary to achieve those purposes;
- e. Ensure that any transfer of research data outside of Canada complies with relevant legislation and that appropriate safeguards are in place to protect the privacy and security of the data;
- f. Ensure that research participants are informed of the purposes for which their data will be used, the organizations or individuals who will have access to it, and any risks associated with the collection, use, or disclosure of their data.

## Procedures

### 1. Data Collection and Use

Research data must be collected and used only for the purposes of the research project and in compliance with applicable legislation, including PIPA, FOIP, and HIA.

- a. Any additional use or disclosure of research data must be consistent with the original purpose for which the data was collected, unless explicit consent has been obtained from the research participant;
- b. ACATCM will provide appropriate notification to research participants regarding the collection, use, and disclosure of their data, including any risks associated with such activities.

### 2. Data Security and Storage

- a. All research data must be stored in secure locations, whether physical or electronic, to protect against unauthorized access, use, or disclosure;
- b. Access to research data will be restricted to authorized personnel only, with appropriate levels of access granted based on job requirements and need-to-know;
- c. ACATCM has implement appropriate technical and administrative safeguards to protect research data, including secure data storage, firewalls, encryption, and access controls;
- d. Research data stored on portable devices such as laptops or mobile phones must be encrypted to prevent unauthorized access in case of loss or theft;
- e. Research data must be securely disposed of when it is no longer required for the purposes of the research project or as required by law.

### 3. Data Sharing and Disclosure

- a. ACATCM will ensure that research data is shared only with authorized personnel or entities for the purposes of the research project, and only to the extent necessary to achieve those purposes;
- b. ACATCM will obtain written agreements from third-party entities with whom research data is shared, ensuring that they will comply with all applicable legislation and provide appropriate safeguards to protect the privacy and security of the data.

## Related Policies

- Privacy Policy