

Policy	Accountability
--------	----------------

Created date:	<DATE>
Applies to:	All Employees, Contractors and Volunteers
Approved by:	<PRIVACY OFFICER>

Purpose

The Accountability Policy of the CIE outlines the Organization's commitment to being accountable to its members, stakeholders, and the community. This policy aims to establish guidelines for transparency, ethical conduct, and responsiveness to the needs and concerns of all stakeholders.

Transparency and Ethical Conduct

Financial Transparency: The CIE is committed to financial transparency. Detailed financial statements, including income, expenses, and balance sheets, shall be made available to members and stakeholders annually.

Ethical Conduct: All members and volunteers shall adhere to a code of ethics that promotes honesty, integrity, and responsible behavior in all Organizational activities.

Engagement with Members and Stakeholders

Communication Channels: The CIE shall maintain open lines of communication with members, stakeholders, and the community through regular updates, newsletters, and feedback mechanisms.

Stakeholder Input: Opportunities for members and stakeholders to provide input, feedback, and concerns regarding the CIE's programs and services shall be established and encouraged.

Decision-Making and Governance

Steering Committee: The CIE's Steering Committee shall act in the best interests of the Organization and its stakeholders, making decisions that align with its mission and values.

Conflict of Interest: Policies and procedures to manage and disclose conflicts of interest among committee members and volunteers shall be established.

Access to Records: Members, stakeholders, and the community shall have the right to access specific Organizational records and documents, as allowed by law.

Performance and Impact

Performance Reporting: The CIE shall regularly report on its performance, including the outcomes and impact of its programs and services.

Evaluations: Program evaluations, privacy impact assessments (PIAs), and audits shall be conducted as needed to ensure the CIE is meeting its goals and objectives effectively.

Community Engagement

Community Involvement: The CIE shall actively engage with the local community and collaborate with partners and other stakeholders to address social service needs.

Feedback and Concerns

Complaint Mechanism: A clear mechanism for members, stakeholders, and the community to submit complaints or concerns about the CIE's actions or services shall be established.

Investigation and Resolution: All complaints and concerns shall be investigated promptly and resolved transparently and fairly.

Policy	Bring Your Own Device (BYOD)
--------	------------------------------

Created date:	<DATE>
Applies to:	All Employees, Contractors and Volunteers
Approved by:	<PRIVACY OFFICER>

Purpose

The purpose of this BYOD policy is to establish guidelines for employees, contractors, and volunteers who wish to use their personal devices (such as smartphones, tablets, or laptops) for work purposes, especially in contexts where sensitive information, including health data and participant information, may be accessed or stored.

Scope

It covers the handling of:

- Personal health information (PHI)
- Personally identifiable information (PII)
- Sensitive client data
- Internal organizational documents and communication

Approval and Registration

All personal devices used for work purposes must be approved by the IT administrator or Privacy Officer.

Employees must register their device with the agency's IT department prior to use.

Approval will be contingent on the device meeting security and software standards outlined in this policy.

Security Requirements

Users must adhere to the following security practices:

- **Encryption:** Devices must have full-disk encryption enabled.
- **Authentication:** Devices must use a strong passcode, biometric lock, or two-factor authentication (2FA).
- **Automatic Locking:** Devices must be set to lock automatically after a period of inactivity (maximum 5 minutes).
- **Software Updates:** Operating systems and apps must be updated regularly to the latest supported versions.
- **Antivirus/Malware Protection:** Must be installed and actively running on the device.

Data Access and Storage

Access to health data or client information must occur only through secure, encrypted channels (e.g., VPN, secure web portal).

No sensitive data may be stored locally on personal devices unless explicitly authorized and encrypted. Use of cloud storage services (e.g., Google Drive, Dropbox) for client or agency data is prohibited unless pre-approved.

Use Restrictions

Users may not share their device with unauthorized individuals (e.g., family or friends) if work data is accessible.

Social media, messaging apps, or other non-work platforms may not be used to share or discuss client or agency information.

Monitoring and Privacy

The CIE reserves the right to monitor, audit, or restrict access to agency systems from personal devices.

The CIE will not access personal data (e.g., photos, messages) unrelated to work.

In the event of a data breach or suspected breach, the agency may require inspection or temporary confiscation of a device.

Incident Reporting

Lost or stolen devices must be reported immediately upon discovery.

Any suspected unauthorized access or data breach must be reported immediately to the Privacy Officer.

Termination or Role Change

Upon termination of employment or role change, users must:

- Remove all work-related data from their personal devices
- Return any installed agency software or credentials
- Cooperate with remote wipe procedures if required

Acknowledgement

All users must sign a BYOD Agreement Form acknowledging they understand and agree to comply with the policy.

Policy	Change Management
--------	-------------------

Created date:	<DATE>
Applies to:	All Employees, Contractors and Volunteers
Approved by:	<PRIVACY OFFICER>

Purpose

The purpose of this policy is to establish a systematic approach to identify, evaluate, and implement changes in the CIE. This policy ensures that changes do not compromise data quality and security.

Change Request Process

Submission of Change Requests:

- Anyone within the CIE may submit a Change Request when they identify a need for changes to the CIE structure or data models.
- Change Requests should be documented using the designated form, which includes a detailed description of the proposed change, the rationale for the change, and its potential impact.

Change Request Review:

- The Steering Committee is responsible for reviewing and evaluating Change Requests.
- The Steering Committee will assess the feasibility, impact, risk and alignment of the proposed change with the CIE's mission and objectives.
- The committee will consider data integrity, security, and any relevant legal and ethical considerations during the evaluation process.

Approval and Documentation:

- Approved changes will be documented with clear instructions and a timeline for implementation.
- The committee will communicate approval to the requestor and other relevant stakeholders.

Change Implementation

Change Implementation Team:

- An implementation team shall be designated to execute approved changes.
- The team should include individuals with expertise in data management and the CIE operations.

Testing and Validation:

- Before changes are deployed to the production environment, they must be thoroughly tested to ensure that they do not introduce errors, vulnerabilities, or compromise data integrity.
- Data validation procedures should be performed to confirm that the changes have the intended impact.

Communication:

- All changes should be communicated to relevant stakeholders, including data contributors, participants, and users of the CIE.

Monitoring and Audit

Ongoing Monitoring:

- The committee shall monitor the changes post-implementation to ensure they do not negatively affect data integrity.

Regular Audits:

- Periodic audits of the CIE will be conducted to identify potential issues or areas for improvement.

Privacy Impact Assessments:

- A Privacy Impact Assessment will be conducted to assess risk and plan mitigation before implementation of a new data field.

Compliance with Applicable Regulations

The CIE will ensure that all change management activities adhere to relevant privacy and data protection regulations, including Alberta's privacy legislation, and any other applicable federal or provincial laws.

Ethical Consideration

The CIE will ensure that ethical consideration is given to any new data elements introduced before implementing change.

Policy	Code of Ethics
--------	----------------

Created date:	<DATE>
Applies to:	All Employees, Contractors and Volunteers
Approved by:	<PRIVACY OFFICER>

Purpose

This Code of Ethics was established to guide the behavior and decision-making of the members and volunteers of the CIE. The CIE is dedicated to serving the community, promoting its mission, and upholding the highest standards of integrity, transparency, and accountability.

Commitment to the Mission and Stakeholders

Vision-Centered Decision Making: Members and volunteers shall make decisions that align with the vision and values of the CIE and prioritize the best interests of the community and stakeholders.

Transparency: The CIE is committed to open and honest communication with stakeholders. Information about programs, finances, and operations shall be readily available to the public, unless confidentiality is legally required.

Fiduciary Responsibility

Stewardship: Members of the Steering Committee shall act as responsible stewards of the CIE's resources, including financial assets, property, and intellectual property.

Conflict of Interest: All conflicts of interest shall be disclosed, and actions taken to avoid conflicts of interest shall be in the best interest of the CIE. Members and volunteers shall not use their positions for personal gain.

Professional Integrity

Honesty and Integrity: All members and volunteers shall act with honesty, fairness, and integrity in all their interactions on behalf of the CIE.

Professional Development: Members of the Steering Committee shall engage in ongoing professional development to enhance their skills and knowledge to better serve the CIE's vision.

Privacy and Confidentiality

Confidentiality: Members and volunteers shall protect the confidentiality of all sensitive and proprietary information related to the CIE, its beneficiaries, and stakeholders.

Non-Discrimination and Inclusivity

Equal Opportunity: The CIE is committed to diversity, equity, and inclusion. Members and volunteers shall not discriminate against any individual or group on the basis of race, color, religion, gender, sexual orientation, age, national origin, disability, or any other protected characteristic.

Accountability and Responsibility

Accountability: Members and volunteers are accountable for their actions and decisions, both individually and collectively. They shall accept responsibility for their mistakes and work towards corrective action.

Advocacy and Public Engagement

Advocacy: The CIE may engage in advocacy efforts to further its mission. Members and volunteers shall adhere to legal and ethical standards when participating in such activities.

Compliance with Laws and Regulations

Legal Compliance: All activities of the CIE shall comply with relevant laws and regulations. Members and volunteers shall strive to ensure that the CIE operates within the bounds of the law.

Reporting Violations

Reporting Concerns: Any member or volunteer who becomes aware of a violation of this Code of Ethics or other unethical behavior within the CIE shall report it to the appropriate authority within the CIE.

Policy	Collection, Use, and Disclosure of Health Information
--------	---

Created date:	<DATE>
Applies to:	All Employees, Contractors and Volunteers
Approved by:	<PRIVACY OFFICER>

Principles

The CIE will not collect, use, or disclose individually identifying health information if aggregate or other non-identifying health information is adequate for the intended purpose.

When collecting, using, or disclosing health information, The CIE will only collect, use, or disclose the amount of health information that is essential to enable the CIE or the recipient of the information to carry out the intended purpose.

Before using or disclosing health information, the CIE will make a reasonable effort to ensure that the information is accurate and complete.

Collection and use of identifying personal and health information

The CIE will not use identifying personal or health information to market any service for a commercial purpose or to solicit money without the expressed consent of the individual who is the subject of that information.

Personal and health information will be collected directly from the individual it is about or his/her authorized representative unless indirect collection is authorized by provincial or federal legislation. Examples of indirect collection are:

- When the individual authorizes collection from a third party (this authorization can be verbal)
- When the individual is unable to provide the information, and the agency/custodian collects the information from an authorized representative of the individual
- When direct collection would compromise the interests of the individual, the purpose of the collection, the accuracy of the information, or the safety of another person (e.g., a patient is not completely truthful or cannot remember information)
- When direct collection is not reasonably practicable (e.g., due to a language barrier or cognitive impairment)
- When information is collected from another agency/custodian during referral or consultative processes
- When the information will be used for a purpose authorized for agency/custodian use under provincial and federal legislation, including data matching

When collecting personal or health information directly from an individual, the CIE will inform the individual of the purpose for which the information is collected, the legal authority for the collection and

the title and business contact information of a staff member who can answer questions. Notification will be provided by means of a sign or verbally (from the agency/custodian) as appropriate.

The use of individually identifying personal or health information in the custody or control of the agency/custodian(s) can be used for the following purposes:

- Providing services (health or otherwise)
- Determining or verifying the eligibility of an individual to receive a service
- Conducting research or performing data matching or other services to facilitate another person's research (research must be approved by a Research Ethics Board)
- Providing for health services provider education
- Carrying out any purpose authorized by an enactment of your Province or Canada
- For internal management purposes, including planning, quality improvement, monitoring, audit, evaluation, reporting, or obtaining or processing payment for health services and human resource management.

The use of the CIE's electronic medical record or other electronic applications may be monitored to ensure appropriate confidentiality, and security. Audit and access logs will be checked by the CIE system administrator periodically and/or if a breach of security or privacy is suspected.

A participating agency/custodian and/or authorized affiliate may access and use information in Netcare if, and only when:

- They are in a current care relationship with the individual who is the subject of the information;
- They are providing health services to the individual either in the presence or absence of that individual;
- Their access to the information is necessary for the provision of the health services or for making a determination for a related health service; and
- The information is related to and necessary for the current session of care.

Unless alternate use or disclosure is authorized, or required by law, or with the knowledge and consent of the subject individual, individuals have the right to request the Information and Privacy Commissioner to review access, privacy, and correction decisions made by the CIE.

Disclosure of personal and health information

The CIE may disclose individually identifying personal and health information to the individual who is the subject of the information or to his / her authorized representative.

Individually identifying personal or health information may be disclosed to a person other than the subject individual, *if the individual has consented to the disclosure or without consent as allowed per provincial legislation provisions.*

The CIE requires written consent from the individual to disclose identifying personal or health information to anyone other than the individual or his / her authorized representative, or to another agency/ custodian. Consent must be provided in writing or electronically and must include:

- the information to be disclosed;
- the purpose for which the information may be disclosed;

- the identification of the agency receiving the information;
- an acknowledgement that the person providing the consent is aware of the reasons why the personal or health information is needed, and the risks and benefits of either consenting or refusing to consent;
- the date the consent is effective and expiry date (if any); and
- a statement advising the person that they may revoke the consent at any time.

In deciding how much information to disclose, an agency/custodian must consider as an important factor, any expressed wish of the individual who is the subject of the information relating to disclosure of the information, together with any other factors the agency/custodian considers relevant.

In all cases, the CIE will disclose the least amount of identifying personal or health information at the highest level of anonymity that the agency/custodian considers necessary to fulfill the request.

The CIE may disclose individually identifying personal or health information without the consent of the subject individual to the following recipients. A notation of the disclosure will be made in the chart.

- To another agency/custodian or affiliate for legally authorized uses
- To a person who is responsible for providing continuing care and treatment to the individual
- To family members of the individual or a close personal friend, if the information is provided in general terms and concerns the presence, location, and condition of the individual on the day on which the information is disclosed
- To contact family members or a close personal friend of the individual, if the individual is injured, ill, or deceased.
- To comply with a subpoena, warrant, or court order.
- If the disclosure is authorized or required by provincial legislation.
- For the purpose of a court proceeding or proceeding before a quasi-judicial body to which the Centre is a party
- To the successor custodian or the attending physician.
- To a health professional body for the purpose of an investigation, discipline proceeding, CIE review, or inspection
- To a researcher who has signed a written agreement with the CIE, in accordance with provincial legislation, and has provided the CIE with a copy of the Ethics Board's response to the research proposal

An agency/custodian that discloses a record containing individually identifying diagnostic, treatment, and care information without the participant's consent **must** make a notation of the disclosure. This notation must be maintained for 10 years.

Disclosure to Protect Public Health and Safety

Discretionary disclosure of individually identifying personal or health information to the police or Minister of Justice and Attorney General where an agency/custodian reasonably believes the information relates to the possible commission of an offence under a statute or regulation of Alberta, and that the disclosure will protect the health and safety of individuals.

The personal or health information the agency/custodian may disclose is:

- the individual's name
- the individual's date of birth
- the nature of any injury or illness of the individual
- the date on which a health service was sought or received
- the location of where the health service was sought or received
- whether any samples of bodily substances were taken from an individual

Disclosure to Prevent or Limit Fraud or Abuse of Health Services

Discretionary disclosure to the police or to the Minister of Justice and Attorney General under provisions of provincial legislation where the agency/custodian reasonably believes the disclosure will prevent or limit fraud or abuse of health services and the disclosure will detect or prevent fraud or limit abuse in the use of health services.

For individuals suspected of fraud or abuse of the health system, the health information that may be disclosed is:

- the individual's name
- the individual's date of birth
- the individual's health number
- the nature of any injury or illness of the individual
- the date on which a health service was sought or received
- the location where the health service was sought or received
- the name and the date of any drug provided or prescribed to the individual

When individually identifying health information is disclosed without the consent of the individual in any of the above circumstances, the name of the person who received the information, the date and purpose of the disclosure, and a description of the information disclosed will be recorded. This record of disclosure must be retained for 10 years.

Authentication of the Recipient

The CIE staff shall take reasonable steps to ensure the disclosure is made to the person authorized and intended to receive the information. This involves verifying and authenticating the identity of any individual to whom health information is disclosed prior to disclosure.

Examples of proof of identity are:

- photo identification (e.g., a drivers licence, passport, etc.)
- a health card
- organization name tag
- business card

Other methods of authenticating include confirming the FAX number provided before sending and confirming that the FAX was received by the intended recipient.

Notation and Notification

When a record containing individually identifying diagnostic, treatment, and care information is disclosed without consent in accordance with provincial legislation, the CIE will record the following information in the participant's electronic record:

- the name of the person to whom the information is disclosed
- the date and purpose of the disclosure
- a description of the information disclosed

When individually identifying diagnostic, treatment and care information is disclosed to anyone other than the individual themselves or another agency/custodian with or without consent, the CIE will inform the recipient in writing of the purpose of the disclosure and the authority under which the disclosure is made.

Policy	Conflict of Interest
--------	----------------------

Created date:	<DATE>
Applies to:	All Employees, Contractors and Volunteers
Approved by:	<PRIVACY OFFICER>

Policy Statement

All members of the CIE are required to perform the duties and activities of their position with the highest level of integrity and independence, in a professional and ethical manner. They must also ensure that they avoid or eliminate any conflict of interest or situation that could reasonably be perceived as a conflict of interest and immediately report it to the Executive Director.

Although this policy details certain behaviors that may lead to a conflict of interest or the appearance of a conflict of interest, it is impossible to anticipate all situations that could lead to one. Members may also inadvertently find themselves in a situation that leads to or could be perceived as a conflict of interest. These situations must also be disclosed.

Compliance with this policy is a condition of involvement. Failure to comply with these provisions may result in disciplinary action, up to and including termination of individual membership.

Action or Behaviors to Avoid

Below, you will find some situations, behaviors or events that should be avoided at all costs by members or other contractual third parties doing business with the CIE.

Personal Interest

Members must ensure that no conflict exists or could appear to exist between their personal interests and those of the CIE's potential partners, vendors, suppliers or other business entities in which you have a direct or indirect financial interest.

Members must not:

- Take part in or attempt to influence any of the CIE's decision or any business dealings with a current or potential partner, vendor, supplier or other business entity in which you have a direct or indirect financial interest
- Use the premises, equipment, supplies or services of other members of the CIE to promote their personal interests;

- Use confidential information for their personal benefit during or after involvement with the CIE;
- To be in a position where they could benefit directly or indirectly from a CIE business or data transaction (e. g. supplier of goods or services, contract, license or partnership);
- Give preferential treatment to any supplier or other person in partnership with the CIE in order to serve their personal interests;
- Invest in, own, have an interest in, or be an employee of an organization that might have an interest, direct or indirect, in any CIE commercial transaction, except in the case of a widely held public company whose dealings with the CIE do not represent a substantial portion of its total business;
- This should not be interpreted as an exhaustive list of all circumstances that could lead to a real or perceived conflict of interest.

Family, Friends

Members must not:

- Use their position or contacts at the CIE to promote their personal interests or those of a family member or person with whom they have a close personal or professional relationship;
- Take part in or attempt to influence any CIE-related decision or business dealings (including those concerning current or potential partners, vendors or suppliers) that may benefit or appear to benefit a relative, close personal friend or a business enterprise in which a relative or close personal friend is involved or has a direct or indirect financial interest.
- The CIE generally does not permit work situations where a member directly or indirectly manages a relative or a person with whom he/she has a romantic relationship. If you are aware that the CIE plans to enlist or employ your relative or a person for a position with whom you have a romantic relationship that directly or indirectly reports to you, you must disclose that information immediately.

Relationships and Favoritism

Members shall not grant or appear to grant preferential treatment to a person with whom they have a close personal or professional relationship. In some situations, past relationships may also give rise to a perceived conflict of interest and should be treated as such.

If a member is in a situation where he or she could make a decision (e. g. evaluation, discipline, promotion, reward, any other form of discretionary control or the awarding of a contract) involving, directly or indirectly, a person with whom he or she has a close personal or professional relationship, the member must:

- Disclose the potential conflict to the Steering Committee
- Refer the decision to the committee or someone designated by them
- Refrain from making any recommendations or conveying views related to the decision.

Outside Business Activities

- Members are permitted to engage in outside employment or activities as long as, and to the extent that;
- It does not compete with or reflect adversely on the CIE or give rise to a conflict of interest.
- It does not engage in any outside activity that is likely to involve disclosure of the CIE's proprietary information.
- It could not be reasonably perceived as compromising the integrity, independence and impartiality expected from the COE or bring the CIE into disrepute;
- It does not inappropriately exploit the member's connection with the CIE;
- Members are permitted to act as board members of an organization external to the CIE, if their participation meets the criteria above, and if authorized by the Steering Committee beforehand.
-

You are not required to seek approval of the following activities:

- Any affiliation with a trade association, professional association or other such organization related to your work or position at the CIE.
- Participation in non-profit civic or charitable activities, including serving as a member of a board of directors or technical advisory board. However, you must obtain approval if the entity is a CIE partner.

If the committee considers the outside activity to be inappropriate, considering the criteria mentioned above, it must inform the member in writing and the individual must avoid, discontinue or modify his/her participation in such activities accordingly. Disclosures and their assessment by the committee must be documented.

Gifts, Hospitality, and Other Benefits

Accepting a gift, a benefit or an offer of hospitality for oneself or for a colleague, family member or friend can lead to uncomfortable situations or to real or perceived conflicts of interest.

Procedure	Correction or Amendment of Personal and Health Information
-----------	--

Created date:	<DATE>
Applies to:	All Employees, Contractors and Volunteers
Approved by:	<PRIVACY OFFICER>

When an individual or authorized representative asks for a correction of factual information and can substantiate that the information is incorrect, the CIE will make the correction to the record.

Examples: name, address, telephone number, and other demographic information

An individual may make a request for correction or amendment in writing to the custodian or privacy officer. An individual may request a correction to another person's information only if they are an authorized representative of that individual.

The custodian has **30 days from receipt** of the request to review the records and to **decide whether to grant or refuse the request**. Corrections will only be made to factual information. Corrections cannot be made to professional opinions or observations or to a record that was not originally created by that custodian. Failure to respond within 30 days is deemed as a decision to refuse the request by the custodian.

If a correction or amendment is granted, within 30 days, the custodian must:

- make the correction or amendment;
- give written notice to the applicant that the correction or amendment has been made; and
- notify any person to whom that information has been disclosed during the one-year period prior to the request (unless the custodian believes the applicant will not be harmed by not providing notification to others, and the applicant agrees).

If a correction or amendment is refused, within 30 days, the custodian must give written notice to the applicant that their request is refused and the reasons for that refusal.

The custodian must also tell the applicant that they can either:

- ask for a review of the custodian's decision by the Privacy Commissioner; or
- submit a statement of disagreement within 30 days of not more than 500 words that describes the requested correction or amendment and the applicant's reason for disagreeing with the custodian's decision.
- If the applicant provides a statement of disagreement, it will be placed on the individual's record and copied to any person whom the custodian has disclosed the record to in the previous 12 months.

Policy	Data Stewardship
--------	------------------

Created date:	<DATE>
Applies to:	All Employees, Contractors and Volunteers
Approved by:	<PRIVACY OFFICER>

Purpose

The Data Stewardship Policy outlined below is established by the CIE to govern the stewardship and management of data contributed by various agencies, recognizing that the individuals we serve maintain ownership of their data. This policy ensures that data is treated with the utmost respect, confidentiality, and security, while providing guidelines for access, use, and protection.

Data Ownership and Custodianship

Data Ownership: The CIE recognizes that the data contributed by agencies remains the property of the individuals represented within the data. Individuals maintain ownership rights and decision-making authority over their data.

Custodianship: The CIE assumes custodianship of the data, meaning that it is responsible for the storage, protection, and appropriate use of the data in line with this policy.

Data Stewardship Roles and Responsibilities

Data Contributors: Agencies contributing data to the CIE are responsible for ensuring the accuracy and completeness of the data they provide.

Data Custodian (The CIE): The CIE is responsible for the secure storage, management, and access control of data. This includes data protection, encryption, regular backups, and disaster recovery planning.

Participants: Individuals retain ownership of their data and have the right to access, rectify, or request the deletion of their data in accordance with applicable privacy laws.

Data Access and Use

Access Control: The CIE will implement strict access control mechanisms to ensure that only authorized personnel can access and use the data. Access shall be granted based on job roles and responsibilities.

Data Use: Data can only be used for legitimate purposes that align with the CIE's mission and the purposes for which the data was originally collected. Any additional use requires explicit consent from the participant.

Data Protection and Security

Data Security: The CIE will implement appropriate data security measures to protect data from unauthorized access, alteration, disclosure, or destruction.

Encryption: Data in transit and at rest shall be encrypted to safeguard against data breaches.

Data Breach Response: In the event of a data breach, the CIE will promptly assess and address the situation, notify affected individuals, and report the breach as required by law.

Ethical Data Practices

The CIE and contributing agencies shall adhere to ethical data practices, including but not limited to the principles of transparency, accountability, fairness, and data minimization. Ref: Code Of Ethics Policy

Compliance with Applicable Regulations

The CIE shall comply with all applicable data protection and privacy laws, including Alberta's privacy legislation, and any other relevant federal or provincial laws.

Data Retention and Deletion

Data shall be retained only for the duration necessary to fulfill the purpose for which it was collected, as specified in data retention policies. Once data is no longer required, it shall be securely deleted. Ref: Document Retention and Destruction Policy

Policy	Document Retention and Destruction
--------	------------------------------------

Created date:	<DATE>
Applies to:	All Employees, Contractors and Volunteers
Approved by:	<PRIVACY OFFICER>

Purpose and Scope

The purpose of this Document Retention and Destruction Policy is to establish guidelines for the retention and destruction of Organizational records and documents by the Steering Committee of the CIE. This policy applies to all records, data and documents, whether in physical or electronic format, generated and maintained by the CIE.

General Record Retention Guidelines

The Steering Committee recognizes that different types of records have different retention requirements. Records should be categorized as follows:

- Financial Records: 7 years
- Legal Records: Permanently
- Governance Records (e.g., Bylaws, meeting minutes): Permanently
- Personnel Records: 7 years after termination
- Program Records: 7 years after program closure
- Donor and Fundraising Records: 7 years
- Miscellaneous Correspondence: 3 years
- Participant Records: As required by law or organizational need

Destruction of Records

Records past their retention period should be destroyed in a secure and confidential manner to safeguard sensitive information. Destruction may include shredding, burning, or secure electronic erasure, as appropriate.

Destruction of records should be overseen by the Chair of the Steering Committee, or their designee, and documented to confirm that it has been carried out in accordance with this policy.

Legal Holds and Pending Litigation

If the CIE is aware of any legal proceedings, investigations, or regulatory matters that may require the retention of specific records, those records should not be destroyed until any legal hold or related requirement is lifted.

Electronic Records

Electronic records should be treated with the same retention and destruction standards as physical records. The CIE shall have a system for securely erasing electronic records and ensuring that backups of the records are also securely deleted in accordance with retention schedules.

Exceptions

Any exceptions to this policy, including longer retention periods or special considerations, must be documented and approved by the Steering Committee in advance of record destruction.

Record Preservation

The CIE may choose to preserve certain records that have historical or archival value. These records should be transferred to an appropriate storage facility for preservation.

Policy	Emergency Executive Succession
---------------	---------------------------------------

Created date:	<DATE>
Applies to:	All Employees, Contractors and Volunteers
Approved by:	<PRIVACY OFFICER>

Purpose

This policy is established to ensure a smooth transition of leadership in the event of an emergency or the unexpected departure of the Executive Director or equivalent position within the Steering Committee of The CIE.

Identification of Key Positions

The following key positions are identified for emergency succession planning:

- Executive Director

Succession Plan

Acting Executive Director:

- In the event of an emergency or unexpected departure of the Executive Director, the Steering Committee shall designate a suitable individual within The CIE to serve as the Acting Executive Director.
- The Acting Executive Director will temporarily assume all responsibilities and duties of the Executive Director until a permanent replacement is found or the emergency situation is resolved.

Selection Criteria:

- The Acting Executive Director shall be selected based on their qualifications, experience, and availability.
- The Steering Committee may choose an existing committee member to serve as the Acting Executive Director, or they may consider appointing an interim Executive Director if necessary.

Communication

Internal Communication:

- The Steering Committee and staff shall be informed of the emergency situation and the appointment of the Acting Executive Director as soon as possible.

- Clear lines of communication shall be established to ensure that all members of The CIE are informed and updated throughout the succession process.

External Communication

- The CIE will also inform relevant external stakeholders and partners about the situation and the appointment of the Acting Executive Director.

Search for Permanent Replacement

Initiating the Search:

- In the event of a permanent vacancy in the Executive Director position, the Steering Committee will initiate a search for a suitable permanent replacement.

Selection Process:

- The Steering Committee will follow The CIE's regular appointment process to find the most qualified candidate.

Policy	Incident and Breach Response
--------	------------------------------

Created date:	<DATE>
Applies to:	All Employees, Contractors and Volunteers
Approved by:	<PRIVACY OFFICER>

Purpose

This policy outlines the procedures for identifying, managing, reporting, and mitigating privacy breaches and security incidents involving personal or sensitive information in the custody or control of the CIE.

Definitions

Privacy Breach: Unauthorized access to, collection, use, disclosure, or loss of personal or sensitive information.

Personal Information (PI): Information about an identifiable individual, including name, contact details, financial, social, or case management records.

Sensitive Information: Includes but is not limited to health, financial, legal, and child protection information.

Custodian: The agency or individual responsible for the information.

Affiliate: Any employee, volunteer, or contractor acting on behalf of the custodian.

Duty to Notify

Affiliate's Duty to Notify

Any employee, volunteer, or contractor who becomes aware of a potential or confirmed privacy breach must notify their supervisor or the designated Privacy Officer immediately or as soon as practicable.

Custodian's Duty to Notify

Upon confirmation of a breach where there is a real risk of significant harm to an individual, the Privacy Officer must notify:

- The affected individual(s)
- The Office of the Information and Privacy Commissioner of Alberta (if required)
- Any relevant oversight body or funding agency, depending on contractual obligations

Assessment of Risk of Harm

The Privacy Officer will conduct a risk assessment to determine whether notification is required. The following factors will be considered:

- Whether the information was accessed or disclosed
- Whether there is reason to believe the information has or may be misused
- Risk of identity theft, fraud, or other harm
- Sensitivity of the information involved (e.g., child welfare, health, housing status)

- Whether the breach could cause reputational, mental, physical, or financial harm
- Whether the information was encrypted or securely protected
- Whether the loss occurred under secure conditions (e.g., locked vehicle, password protection)
- Whether the breach has impacted service delivery

Incident Response Procedure

Immediate Containment: Limit the exposure of the breach (e.g., shut down system access, recover lost documents).

Notification to Privacy Officer: Report details of the incident including time, scope, persons affected, and actions taken.

Initial Investigation: The Privacy Officer will initiate a breach report and investigate cause, extent, and corrective measures.

Risk Assessment: Determine whether the incident meets criteria for reporting to authorities and affected parties.

Notification (if required): Provide timely written notice to affected individuals, including:

- What happened
- What information was involved
- Steps taken by the agency
- Recommended actions for the individual
- Contact for further inquiries

Report to Authorities: If applicable, report the breach to the Office of the Information and Privacy Commissioner (OIPC), funding partners, or other regulatory bodies.

Documentation: Complete an Incident Report Form and retain it in the agency's breach log.

Remediation and Review: Implement corrective actions (e.g., training, policy updates, disciplinary measures).

Notification Content Requirements

- Any breach notification to individuals must be in plain language and include:
- Description of the breach
- The type of information involved
- Potential harms
- Mitigating steps taken
- Support or resources offered
- Contact information for the Privacy Officer

Training and Awareness

All staff and affiliates must complete mandatory privacy and breach response training upon onboarding and annually thereafter.

Policy	Information Handling
Created date:	<DATE>
Applies to:	All Employees, Contractors and Volunteers
Approved by:	<PRIVACY OFFICER>

Purpose

The information security provisions of provincial legislation have the requirement for the CIE to protect individually identifying personal and health information in their custody or control by making reasonable security arrangements to protect against unauthorized access, collection, use, disclosure, or destruction. They also require the CIE to take appropriate safeguards for the security and confidentiality of records, including addressing the risks associated with electronic health records. This procedure outlines administrative, technical, and physical safeguards to protect confidential information and electronic records.

Administrative Safeguards

- The CIE shall ensure that policies and procedures to facilitate the safeguarding of confidential information in its custody or control are developed and maintained. The CIE shall appoint a Privacy Officer, complete a PIA where required when physical, technical, or administrative changes occur for the CIE that affect the collection, use, or disclosure of personal or health information.
- The need for confidentiality and security of information shall be addressed as part of the conditions of joining the CIE and included in the contracts. All who join the CIE must be aware of and appropriately trained in safeguarding information. A review of CIE's privacy and security policies and procedures and agreement with them must be completed by all agencies joining the CIE. A Confidentiality Agreement must be signed at time of being given access to the CIE. The performance of individuals shall be monitored to reduce the risk of error, fraud, or misuse of information.
- The least amount of information necessary for the intended purpose will be used or disclosed, and only with a **need to know**. If the intended purpose can be accomplished without use or disclosure of identifying information, then the information should be made anonymous.
- Anyone using the CIE shall report any violations or breaches of information security as soon as possible to the Privacy Officer in order that corrective action can be taken to resolve the immediate problem and minimize the risk of future occurrence. The nature of the response will be determined according to the level of gravity of the breach / violation and may include dismissal.
- Agencies participating in the CIE who have PMS vendors must have administrative safeguards in place, including, but not limited to, maintaining and monitoring full audit trails, training vendor

and subcontractors on privacy and security awareness, and conducting regular threat risk assessments to ensure risks are identified and mitigated.

Technical Safeguards

- Information system users are assigned a unique identifier (User ID) that restricts access to each data and application systems to that information required for the administration of their duties. Use of user IDs other than that assigned to an individual is prohibited.
- System administrators must have an administrator account for performing system administration.
- Passwords are to be kept confidential at all times and should not be written down, posted publicly, or shared with other staff except for security purposes. Unique passwords or other authentication controls are required for each desktop, network, server, PMS, etc. A strong password standard is used. Passwords for the PMS is changed every 90 days, as prompted by the system.
- All monitors used to display identifying personal or health information will time out after 5 minutes of inactivity and require entry of a password to reactivate the screen. Staff are to log-off or lock workstations then they leave them unattended to prevent unauthorized access, especially in patient or public areas. All computers are logged off and/or shut down at the end of the business day where applicable.
- Confidential business or identifiable health information will not be sent via e-mail over public or external networks without the use of appropriate security measures such as encryption or by the use of a two-factor authentication connection.
- To detect unauthorized access and prevent modification or misuse of user data in applications, use of internal network will be monitored by the System Administrator and ensure conformity to access policies and standards. Audit and access logs will be checked by the system administrator if a breach of security or privacy is suspected.
- Role based access is used. Access to information is based on an individual's roles and responsibilities.
- Each user should have a unique user login and password to access the computer network. User rights and accounts will be assigned and maintained by the CIE administrator. Installation or alteration to system software and hardware will be the responsibility of IT and the Privacy Officer. The Privacy Officer will ensure that original master copies of software are stored with proper physical controls.
- All electronically stored participant data meets the physical, administrative, and technical safeguards outlined in our policies.
- The CIE's administrative data (e.g. emails, contact lists, Microsoft documents, etc.) will be backed up daily using an encrypted method (e.g. encrypted hard drive, encrypted cloud based back-up)

- The CIE's PMS vendors have a consistent patch management process in place for its network and workstation operating systems. Patches are applied regularly with critical patches applied as soon as they are released.
- Laptops and mobile devices (PDA's, memory sticks, etc.) require layered security protection. CIE participants using laptops will be provided specific training on mobile computing to ensure that they understand the physical, administrative, and technical safeguards implemented. These include:
 - Ensuring that the Administrator account has been renamed and given a strong password.
 - Never leaving the laptop computer unattended, particularly overnight on desktops. Lock it in a desk drawer or cupboard.
 - Selecting laptop computers that have hard drive (power on) passwords and use these protection measures. Passwords on the hard drive boot sector are more secure than operating system user passwords.
 - Not storing personal or health information on mobile computing devices unless needed.
 - Encrypting individually identifying health information data on the hard drive as well as data on all other mobile devices.
 - Each laptop computer will have a personal firewall installed. Firewalls are not to be turned off by the user; the firewall will be password-protected so that only the network administrator can change it. Users are to request the network administrator to change settings on a firewall when required.
 - Ensuring that the laptop computer's network connection defaults are set to disable automatic roaming.
 - Mobile devices must have at minimum, unique password settings and, where possible, data encryption enabled.

Physical Safeguards

- All records will be held and stored in an organized, safe and secure manner.
- Identifying personal or health information will not be displayed or left unattended in public areas. Computer monitors are positioned so that on-screen information cannot be viewed by the general public or have a privacy screen.
- Identifying health information that is transported between agencies, or third parties will be sealed, marked as confidential, and directed to the attention of the authorized recipient.
- CIE participants will verify the credentials and identity of courier services used to transport health information.
- All fax transmissions will be sent with a cover sheet that indicates the information being sent is confidential and giving a telephone number to call if received in error. If preprogrammed

numbers are used, a test fax will be sent to each number to verify accuracy before entering that number in the address book. Reasonable steps will be made to confirm that confidential information transmitted via fax is sent to a recipient with a secure fax machine and that fax numbers are confirmed before information is transmitted.

- Information that is not confidential or sensitive in nature will be disposed of by placing it in recycling bins and/or shredded in-house.
- Before destroying records, it is recommended that a list be made of the names of the participants whose records are to be destroyed, and that this list be kept permanently in a secure location. The purpose is to be able to later determine at a glance that a record has been destroyed and has not simply been lost or misplaced.
- Wireless computer connections are used.
- Prior to disposal of electronic storage devices (e.g. computers, hard drives, CDs), the media will be destroyed by IT Support under the direction of the privacy officer so as to be unusable.
- Patient health information, in any format (hard copy or electronic), is retained for a minimum of 10 years following the last documented contact with the patient or, in the case of a minor patient, 10 years past the age of majority in Alberta.
- Transitory records are documents that are required for routine or short-term transactions and contain little or no information of ongoing value. Due to this level of value, these documents should be discarded. This may include temporary information (records required for specific activities but having no further value once the activity has been completed e.g. phone messages, post-it notes). Types of transitory records:
 - **Temporary information**, such as phone messages, voice mails, post-it notes, invitations and cover sheets.
 - **Duplicates** – exact copies of records maintained as master copies and that have not been altered or added to in any way. Includes photocopies and paper or voice records scanned into or entered into the electronic medical record.
 - **Direct mail**, including unsolicited mail, brochures, etc. from outside sources.
 - **Blank information media**, including unused forms, tapes, etc.
 - **Draft documents**, including source materials used in preparation of documents, draft reports, earlier versions of completed documents. Be sure that draft documents of the following types of records are no longer required for future accountability and documentation purposes:
 - Legal agreements
 - Policies, standards, and guidelines
 - Medical or scientific studies

Policy	Membership and Termination
--------	----------------------------

Created date:	<DATE>
Applies to:	All Employees, Contractors and Volunteers
Approved by:	<PRIVACY OFFICER>

Introduction

The CIE was established to facilitate data sharing and collaboration among participating agencies to enhance service delivery and improve outcomes for individuals and families in Alberta. This policy outlines the requirements for joining, contributing, and terminating participation in the CIE.

Purpose and Scope

This policy aims to provide guidelines for:

- The eligibility criteria and requirements for organizations seeking to join the CIE.
- The responsibilities and obligations of participating agencies contributing data to the CIE.
- The process for voluntary withdrawal from the CIE.
- The process for terminating participation due to non-compliance or inactivity.

Eligibility and Requirements for Joining

To join the CIE, Agencies must meet the following eligibility criteria and requirements:

Eligibility:

- The Agency must be a registered non-profit social service agency operating in Alberta.
- The Agency must have a legitimate need for the data within the CIE to improve service delivery and outcomes for individuals and families.

Privacy Maturity Capacity:

- Joining Agencies must demonstrate a maturity Level 3 or higher as assessed by the Privacy Maturity Capacity Assessment Tool.

Data Sharing Agreement:

- Agencies must sign a Data Sharing Agreement (DSA) that outlines the terms and conditions for data sharing, including data privacy, security, and usage policies.

Data Compatibility:

- Agencies must ensure that their data systems are compatible with the CIE's technical specifications for data submission.

Data Quality and Accuracy:

- Agencies must commit to maintaining the quality and accuracy of data shared with the CIE.

Data Contribution

Data Sharing Protocol:

- Participating agencies must adhere to the Data Sharing Agreement and follow the established data sharing protocol to submit relevant data to the CIE.

Timely Submission:

- Data must be submitted in a timely and consistent manner, as specified in the data sharing protocol, to ensure data currency and accuracy.

Data Privacy and Security:

- Data shared must adhere to strict data privacy and security measures, as outlined in the Data Sharing Agreement.

Termination of Participation

Voluntary Withdrawal:

- An agency may voluntarily withdraw from the CIE by providing written notice to the CIE Steering Committee with at least 30 days' notice.

Non-Compliance and Inactivity:

- The CIE may terminate an agency's participation if it fails to comply with the terms of the Data Sharing Agreement, or if the agency becomes inactive for an extended period.

Data Retention

- Upon termination, data contributed by a participating agency may be retained for a specified amount of time for historical, reporting, or research purposes.

See Document Retention and Destruction Policy

Dispute Resolution

- Disputes arising from this policy will be resolved in accordance with the dispute resolution mechanisms specified in the Data Sharing Agreement.

Training

To ensure the protection of personal and sensitive data shared through the CIE, all employees, contractors, and volunteers from participating agencies must complete mandatory privacy training as outlined below.

Mandatory Training Requirements:

- All new members (employees, contractors, volunteers) must complete privacy training before being granted access to the CIE system or data.
- Members must acknowledge understanding of and compliance with CIE privacy policies upon completion of training.

Annual Refresher Training:

- All users must complete annual privacy refresher training to maintain continued access to the CIE system.

Tracking and Documentation:

- Each agency is responsible for tracking and documenting training completion for its members and submitting compliance reports to the CIE Privacy Office upon request.
- Non-compliance with training requirements may result in temporary suspension of system access or, in cases of ongoing failure, termination of participation.

Role-Based Training:

- Additional training may be required for individuals with elevated access privileges or specialized roles.

Policy Acceptance

- By joining the CIE and contributing data, agencies acknowledge their acceptance of this policy and all CIE Policies and commit to abiding by them.

Privacy Charter

Created date:	<DATE>
Applies to:	All Employees, Contractors and Volunteers
Approved by:	<PRIVACY OFFICER>

Introduction

The CIE has adopted this Privacy Charter to guide how our organization collects, uses, and discloses personal and health information.

Health Information

Our organization respects the privacy rights of our participants and are committed to protecting the personal and health information that we collect from you. We have adopted this privacy charter to guide how we collect, use and disclose participants personal information to provide services. While participant consent can be granted in an informal way, in some situations we must have formal consent to collect, use, and disclose your personal information.

Principles

Principle 1 - Accountability / Management

We are accountable for the personal and health information that you give to us.

The CIE is accountable for all personal and health information in our possession or control, including any information that we disclose to other custodians or that we are required to share with third parties in order to provide you with services.

We have established policies and procedures aimed at maintaining the privacy of our participants. We have appointed a Privacy Officer to oversee privacy issues for the CIE. We have educated our employees, contractors and volunteers about our Privacy Charter and their role in protecting your privacy. Participants with questions about our privacy practices are free to contact our Privacy Officer.

Principle 2 - Notice

We will explain why we collect individually identifying health information before we collect it.

We explain why we collect your individually identifying personal or health information, and the legal authority that authorizes us to collect it. We will collect individually identifying personal and health information only for the following purposes, or as otherwise permitted by law:

- *Provision of services*
- *Verify eligibility for services*
- *Referral for services*

- *Health-Related Educational Communications* (e.g. appointment reminders, providing information about treatment alternatives, or other health-related benefits and services that may be of interest to you).

Principle 3 - Collection

We limit the amount and type of health information we collect.

The CIE will only collect personal and health information for the purposes that we have identified or as otherwise permitted by law. In addition, we will only collect as much personal and health information as is essential to carry out the purpose for which we are collecting it.

Your personal and health information will be collected directly from you, except in the limited circumstances where we are authorized by PIPA or the HIA to indirectly collect such information.

Principle 4 - Use and Disclosure

We will use and disclose your personal and health information only for the reasons for which it was provided to us, unless otherwise permitted by law.

In providing services to you, we may use your health information within the CIE or may disclose it to other custodians to provide you with services on a need-to-know basis for the purpose it was collected. Any third-party disclosure of information requires your written consent, unless otherwise permitted by law.

Provincial legislation also identifies situations in which the disclosure is mandatory or discretionary. In all cases, we will only disclose as much information as is essential for the purpose it is being disclosed or per provincial legislation requirements.

Some of your health information may be deemed “prescribed health information” and we will be required to make it accessible to authorized custodian via the Alberta Electronic Health Record (EHR) [Alberta Netcare]. Consideration of expressed wishes of the participant will be considered when making your information accessible, and participants can ask for some of their health information to be “masked”. When authorized health service providers access health information in Alberta Netcare it is considered a use of health information, not disclosure.

Principle 5 - Consent

We may disclose your health information to a third party with your written consent to that disclosure.

If you consent to disclosure of your health information, you may revoke that consent at any time per the requirements set out in provincial and federal legislation. The consequences of withdrawal of consent will be discussed with you and documented.

Principle 6 - Access

You have a right to access your personal and health information that is the CIE’s custody or control within the provisions of provincial legislations.

Participants own their personal and health information in their record; the CIE owns the record. During the provision of services, we will share your personal and health information with you or your authorized representative verbally and allow access to or provide copies of your records when practical.

(This includes information in Alberta Netcare).

Each person has the right to review and obtain a copy of their personal information on record at the CIE, with limited exceptions. To find out what information the CIE has about you, contact them in person or in writing. In most instances, they will respond to your request within 30 days

Principle 7 – Safeguards

We will protect your personal and health information from unauthorized access, use, disclosure or destruction.

We have assessed the risks to your personal and health information and implemented administrative, technical and physical safeguards to eliminate or minimize the risk. Examples of these safeguards include office policies and procedures that ensure that your information cannot be seen by unauthorized persons, having employees, contractors and volunteers sign confidentiality agreements to ensure they understand the importance of confidentiality, electronic security mechanisms like firewalls and password protection.

Principle 8 - Quality

We take efforts to ensure the personal and health information in our custody or control is accurate and complete before using or disclosing that information.

We update our registration information as required. We ensure our records are complete and accurate, and track additions and amendments. We correct inaccurate or incomplete factual information.

You are encouraged to advise us of any changes to your personal information that may be relevant to the services we are providing to you. At any time, you can ask us to allow you to review the personal information we have about you and, where necessary, you will be able to update that information to ensure that it is accurate.

Principle 9 - Retention and Destruction of Records

We will retain your personal and health information per the applicable provincial guidelines, and securely destroy of your information when it is no longer needed.

We will keep your personal and health information per provincial record retention guidelines or as long as necessary to accomplish the purpose for which it was collected (whichever is longer).

We destroy paper health information by shredding and destroy or use professional disk wiping software to remove health information from computer hard drives and other media.

Principle 10 – Monitoring & Enforcement

We monitor compliance with our privacy policies and procedures and have a process for handling complaints about the handling of personal and health information.

We regularly assess our personal and health information safeguards, and ensure our staff, contractors and volunteers know what they are and that they follow them. We have put in place sanctions for anyone who breaches or attempts to breach our safeguards to demonstrate the important we place on preserving privacy and confidentiality.

We investigate all privacy complaints or suspected privacy breaches, and take appropriate remedial measures including amending our policies, disciplining staff, etc. Where you believe that your concerns have not been satisfactorily addressed, contact the CIE Privacy Officer directly. The Privacy Officer will ensure that a complete investigation of your complaint has been undertaken and will report their findings to you, in most instances, within 30 days.

We have a process for handling requests for correction or amendments to personal and health information. In the event that a complaint cannot be resolved, the CIE Privacy Officer will advise the individual of the mechanism for referral of the complaint to the applicable provincial College, or the Office of the Information and Privacy Commissioner.

Personal Employee Non-Health Related Information

The CIE also respects the privacy rights of our employees, contractors and volunteers and is committed to protecting the personal information that we collect from them.

As an employer, we will collect employee's personal information specific to payroll requirements. We will use this information in a way that is reasonable to fulfill our obligations and have taken step to protect the information they provide to us. The type of information may include employee resume, letter of employment / contract, salary or wage history, performance related documents (including performance reviews, commendations, and disciplinary action), and tax forms. We will maintain this information securely. Employees have the right to review their own employee records by contacting the CIE's Privacy Officer.

Procedure	Right of Access
-----------	-----------------

Created date:	<DATE>
Applies to:	All Employees, Contractors and Volunteers
Approved by:	<PRIVACY OFFICER>

Purpose

Subject to limited and specific exceptions in provincial and federal legislation, individuals have a right of access to information about themselves that is in the custody or control of the CIE and the right to request corrections or amendments to this information. The existence of a current care relationship will be jointly determined by the participating staff and the individual.

This procedure is intended to define a process for facilitating requests for access to an individual's health information.

Routine Access to Own Personal and Health Information

- During the provision of services, staff will share information verbally with the participant or authorized representative and allow access to or provide copies of their own records when practical.
- It is preferable to have a participant request access to their own information by submitting a written request to the Privacy Officer.
- The CIE shall provide access to individually identifying personal or health information only to the individual who is the subject of the information or to their authorized representative.
- When access to personal or health information is requested by an individual, it will be documented and dated (Disclosure Log).
- A fee may be applied to formal requests for access to their files by the individual, or the CIE may choose to waive the fee. Regulation sets out the maximum fees that can be charged for providing access.

Formal Request for Access to Information

When participants have not been satisfied with the amount or kind of information that they have received through the CIE's routine procedures, participants may make a **formal request for access** to information in writing.

- An individual may request access to another person's information only if they are an authorized representative.
- All formal requests for access to information will be processed in accordance with procedures set out in provincial legislation. Any health or personal information about individuals other than

the applicant will be severed before disclosure of the records. Requests will be processed within 30 days of receipt.

- All requests for access to information should be directed to the CIE's Privacy Officer.
- After receiving the request, the Privacy Officer will retrieve the requested records and, in accordance with the fee schedules set out in provincial and federal legislation, prepare a fee estimate, or choose to waive the fee.
- Once the fee estimate is prepared, the Privacy Officer will notify the applicant of the cost for providing the information requested. The applicant has up to 20 days to indicate if the fee estimate is accepted or to modify the request to change the amount of the fee assessed.
- Processing a request ceases once a notice of estimate has been forwarded to an applicant and begins again immediately on the receipt of an agreement to pay the fee.
- Once the estimate has been agreed to, the Privacy Officer will review the requested records and, in consultation with appropriate staff, prepare the records for disclosure. All records relating to the request will be reviewed on a line-by-line basis to determine possible exceptions to disclosure.
- Access to personal or health information can only be denied based on mandatory or discretionary exceptions outlined in provincial legislations. Access requests cannot be denied based on the reason for the request. Any health information or personal information about an individual other than the applicant will be severed before disclosure of the records.
- Where the Privacy Officer determines that discretionary or mandatory exceptions apply to the records requested, the excepted information will be removed from the record prior to the record being disclosed to the applicant. The applicant will be advised that information has been excepted from disclosure, and under what sections of provincial legislations the exceptions have been made.

Mandatory exception to the right of access

The CIE **must refuse** access to an applicant:

- where the request is for information about a person other than the applicant, unless the information was originally provided by the applicant in the context of a service being provided to the applicant or the applicant has authority to receive the information (e.g., guardian of a minor, executor of an estate for purposes authorized under provincial legislation).
- where the information sets out procedures or contains results of an investigation, a discipline proceeding, a review, or an inspection relating to a health service provider.
- where disclosure is prohibited by other law of Alberta or Canada.

Discretionary exception to right of access

The CIE **may refuse** access to an applicant if the disclosure could reasonably:

- be expected to result in immediate and grave harm to the applicant's mental or physical health or safety
- be expected to threaten the mental or physical health or safety of another individual
- be expected to pose a threat to public safety

- lead to the identification of a person who provided personal or health information to the CIE explicitly or implicitly in confidence and in circumstances in which it was appropriate that the name of the person who provided the information be kept confidential
- be expected to prejudice the use or results of particular audits, diagnostic tests or assessments

Response to the applicant

A response must be made within 30 days of receipt of the request unless the time limit has been extended, as allowable by law.

As part of the CIE's response, the applicant shall be told:

- whether access to the record or partial record is granted or refused
- if access is granted, where, when, and how access will be given

If access is refused:

- The reasons for refusal and basis of refusal and
- The name, title, business address, and phone number of the Privacy Officer and that the applicant has a right to request a review of the decision by the Office of the Information and Privacy Commissioner of Alberta.

Disclosure of Information to Law Enforcement

Permitted Disclosures to Law Enforcement

The CIE may disclose personal or health information to a police or law enforcement agency *without the individual's consent*:

- When the disclosure is required by a court order, warrant, subpoena, or summons.
- When the disclosure is necessary to prevent or reduce a serious risk of harm to the health or safety of any individual or group.
- When the information is required to assist in locating a missing person.
- When cooperating with a law enforcement investigation or proceeding, and the disclosure is permitted under PIPA, Section 20(g) or HIA, Section 35(1)(i).
- Where required for the enforcement of a law of Alberta or Canada, and the information is necessary for carrying out that investigation or enforcement.

Procedure for Responding to Law Enforcement Requests

- All police or law enforcement requests must be directed immediately to the Privacy Officer.
- The Privacy Officer will review the request to determine if the information can be released:
 - Verify the identity of the requester and confirm the legal authority (e.g., warrant or court order).
 - Assess whether the disclosure meets the permitted criteria.
- The disclosure, if approved, will be documented in the Disclosure Log, including:
 - Date and time of the request and response
 - Name and badge number of the officer

- Legal authority cited for the request
 - Description of the information disclosed
 - A copy of the request (if provided in writing)
- If the request is denied, the Privacy Officer will provide the reason and direct the law enforcement agency to obtain appropriate legal authorization if necessary.

Emergencies

In urgent or emergency situations where time is critical, the Privacy Officer may permit disclosure without prior written documentation if:

- There is a serious and imminent threat to the safety of an individual or the public.
- The information is necessary to prevent harm.

Disclosure log

A file (disclosure log) shall be kept for each request processed:

- All internal and external correspondence, including a copy of the original request from the applicant, any notices sent to the applicant, and any other correspondence from the applicant
- An unmarked copy of the records retrieved and reviewed in response to a request
- A copy of the documents released to the applicant
- Any other information documenting the request management process

A staff member shall be present if the applicant views the original record in order to answer questions and maintain the integrity of the record. If information is severed from the record before disclosure of the information, the applicant no longer has the option of viewing the original record and will view photocopies of the record.

Authentication of recipient

The CIE shall take reasonable steps to verify the identity of the individual or authorized representative before allowing access to disclosing personal or health information. This may involve looking at a driver's license or health card.

An authorized representative is any person who can exercise the rights or powers conferred on an individual under applicable privacy legislation. This includes the right of access to an individual's personal or health information and the power to provide consent for disclosure of such information.

When an authorized representative requests an individual's health information and is not known to the CIE, proof of authority may be requested. This may involve asking for a copy of such documents as a guardianship order, power of attorney, personal directive, or letters of administration for an estate.

Policy	Risk Management
--------	-----------------

Created date:	<DATE>
Applies to:	All Employees, Contractors and Volunteers
Approved by:	<PRIVACY OFFICER>

Purpose

The Risk Management Policy of the CIE is designed to identify, assess, and mitigate risks to ensure the safety of stakeholders, protect assets, and support the continuity of essential services. This policy outlines guidelines for managing risks related to insurance, safety procedures, and emergency planning.

Risk Identification and Assessment

Regular Risk Assessment: The Steering Committee shall conduct regular risk assessments to identify potential risks associated with the CIE's activities, services, and facilities. Risks will be categorized as financial, operational, legal, and reputational. Privacy Impact Assessments will be reviewed annually for needed amendments regarding changes in third-party relationships, as well as changes to collection, use, disclosure or disposal of data.

Risk Evaluation: Risks will be evaluated for their likelihood and potential impact. A risk matrix shall be developed to prioritize risks based on severity.

Insurance Management

Insurance Coverage: The CIE shall maintain appropriate insurance coverage to protect against identified risks. Types of insurance may include general liability, property, members and officers' liability, and professional liability, among others.

Regular Review: The CIE shall regularly review insurance policies to ensure they adequately cover current risks and operations.

Insurance Documentation: Policies and associated documentation shall be maintained, and certificates of insurance shall be kept on file.

Safety Procedures and Practices

Health and Safety: The CIE is committed to providing a safe and healthy environment for volunteers and members. Policies and practices shall comply with applicable health and safety regulations and standards.

Training: Members and volunteers shall receive appropriate training to maintain safe practices and emergency response procedures.

Emergency Planning

Emergency Response Plan: The CIE shall develop and maintain a comprehensive Emergency Response Plan to address potential crises, including natural disasters, security breaches, and other emergencies. This plan shall include evacuation procedures, emergency contacts, and communication protocols.

Testing and Drills: Periodic drills and testing of the Emergency Response Plan will be conducted to ensure preparedness.

Crisis Communications: In the event of an emergency, a crisis communication strategy will be implemented to inform stakeholders, staff, volunteers, and clients of the situation and the Organization's response.

Reporting and Documentation

Risk Reporting: Identified risks and mitigation efforts shall be documented and reported to the Steering Committee. Significant risks shall be escalated as necessary.

Recordkeeping: Records related to risk assessments, insurance, safety procedures, and emergency planning shall be maintained and kept for an appropriate period.

Policy	Treatment and Protection of Users and Participants
--------	--

Created date:	<DATE>
Applies to:	All Employees, Contractors and Volunteers
Approved by:	<PRIVACY OFFICER>

Purpose

The CIE is dedicated to providing high-quality and ethical services to our users and participants. This policy underscores our commitment to safeguarding the well-being, dignity, and rights of all individuals who access our services, or whose data is stored within.

Principles

Respect and Dignity: We are committed to treating all users and participants with respect, dignity, and consideration for their cultural, social, and individual diversity.

Safety: We prioritize the physical and emotional safety of those we serve, ensuring they are protected from harm and abuse.

Autonomy: We support the right of individuals to make informed choices and decisions about the services they receive, respecting their autonomy.

Confidentiality: We uphold strict confidentiality standards, ensuring that personal information shared by individuals remains protected and is used only for authorized purposes.

Quality of Service: We strive for the highest standards of quality in our services, with continuous improvement and a commitment to evidence-based practices.

Participant Rights

Informed Consent: Participants will be provided with clear, understandable information about the services offered and their rights. Informed consent will be sought before providing services. The Participant can also withdraw their consent at any time.

Access to Information: Users and participants have the right to access information about themselves and about the services and policies of the CIE.

Privacy: We will ensure the privacy of individuals' personal information and provide them with a clear understanding of how their data is used and protected.

Non-Discrimination: We do not discriminate based on race, color, religion, gender, sexual orientation, gender identity, national origin, age, disability, or any other protected status.

Complaints and Grievances: Individuals have the right to make complaints or raise grievances about the services they receive, and the CIE will have a process for addressing and resolving these concerns.

Protection from Harm

Abuse Prevention: The CIE is committed to preventing and responding to all forms of abuse or harm that may befall individuals from using our services.

Safety Measures: Adequate safety measures will be implemented to protect individuals from any potential harm associated with our services.

Autonomy and Consent

Decision Making: Individuals have the right to make their own choices and decisions about the services they receive and whom their data is shared with, and the CIE will respect these choices within legal and ethical boundaries.

Incapacity: In cases where an individual is unable to make decisions, the CIE will follow established legal and ethical procedures to protect their rights and best interests.

Confidentiality and Data Protection

Data Protection: Personal information will be collected, stored, and used in compliance with applicable laws and regulations.

Disclosure: Information sharing will only occur as legally mandated or with the informed consent of the individual.

Quality of Service

Continuous Improvement: The CIE will continually assess and improve the quality of services to meet the needs and expectations of individuals.

Compliance and Reporting

Compliance: The CIE shall remain compliant with all relevant laws and regulations, including those specific to the protection and treatment of individuals.

Incident Reporting: The CIE will have a protocol for reporting and addressing incidents related to the treatment and protection of users and participants.

DRAFT

Vendor Assessment Checklist

Vendor Information

Vendor Name	
Vendor Contact • Name • Title • Phone • Email	
Vendor Address	
Vendor Website	

Product/Service Information

Description of Product or Service	
Scope of Use Within the CIE	
Vendor's Role in the CIE's Operations	

Risk Assessment

Identification of Potential Risks: • Operational • Security • Compliance • Financial • Legal • Reputational	
---	--

Impact Analysis: • High • Medium • Low	
Probability of Occurrence: • High • Medium • Low	
Risk Priority: • High • Medium • Low	

Mitigation Strategies	
Define specific actions to mitigate each identified risk.	
Assign responsibilities for risk mitigation.	
Set timelines for mitigation actions.	
Define Key Performance Indicators to monitor mitigation efforts..	

Questions to ask prior to entering into an agreement

- ☐ Have there been past security issues with or criticisms of the tool?
- ☐ If so, how quickly have they responded to criticisms about their tool?
- ☐ How quickly have they patched or made updates to fix vulnerabilities?
Note that criticisms and vulnerabilities are not necessarily a bad sign for the company, as even the most carefully built software can have vulnerabilities. What's more important is that the company takes security concerns seriously and fixes them as quickly as possible.
- ☐ Do you have a plan to stay well-informed on the latest news about the tools that you use?

- ☐ Is this vendor honest about the limitations of their product?
Vendor should be able to clearly state the situations that their security model doesn't defend against.
- ☐ Does the company provide a guarantee about the availability of your data? (SLA)
- ☐ How likely is it that this company is going to stick around? Does it seem like they have sustainable business practices?
- ☐ If the service disappears, is there a way to access your data and move it to another service provider or app? Or will it be gone forever?
- ☐ Is there any chance that they will ban you from using their app or service, and thus also lock you out from accessing your data? *Think about if there are any limits to how the service can be used.*

Questions to ask the vendor

- ☐ Does the vendor have a privacy policy on their website? Do they share or sell data to any third parties?
- ☐ Notification: do they promise to notify us of any legal demand *before* handing over any of our data, or data about us (with no exceptions)?
- ☐ Viewing: Do they promise not to look at our data themselves, except when they absolutely need to?
- ☐ Sharing: Do they require anyone who they share the data with to abide by the same privacy policy and notification terms?
- ☐ Restriction: Are they only using the data for the purpose of which they provided?
- ☐ Will the vendor disclose any client data to their partners or other third parties in the normal course of business? If so, are those conditions clearly stated? What are the privacy practices of those other entities?
- ☐ Does the vendor follow current best practices in responding to government requests in your jurisdiction?
- ☐ Do they require a warrant before handing over user content?
- ☐ Do they publish regular transparency reports?
- ☐ Do they publish law enforcement guides?
- ☐ Do they have a dedicated security team? If so, what is their incident response plan? Do they have any specifics about responding to breaches of data security?
- ☐ Have they had a recent security audit? If there were any security issues found, how quickly were they fixed?

- ☐ How often do they get security audits? Will they share the results, or at least share an executive summary?
- ☐ What measures do they take to secure private data from theft or misuse?
- ☐ Have they had a data breach? *(This is not necessarily a bad thing, especially if they have a plan for how to prevent them in the future. This is really about what was breached— for example, was it a contact list from a webform, or their health information files?)*
- ☐ If they had a data breach in the past, what measures have they taken to prevent a data breach in the future?
- ☐ How does the company notify customers about data breaches?
- ☐ Does the vendor give advance notice when it changes its data practices?
- ☐ Does the vendor encrypt data in transit? Do they default to secure connections?

(For example, does a website redirect an unencrypted HTTP website to an encrypted HTTPS site?)
- ☐ What is the vendor's disaster recovery plan and backup scheme?
- ☐ What internal controls exist for vendor's staff accessing logs, client data and other sensitive information?
- ☐ Does this service allow 2-factor authentication on login? If not, why not? How soon do they plan to implement it?
- ☐ Do they push regular software updates?
- ☐ Do they encrypt stored data? (This is also called "encrypted at rest." For example, when it's "in the cloud"/on their computers, is it encrypted?)
- ☐ Do they have a bug bounty program? If they do not have a bug bounty program in place, how do they respond to vulnerability reports? (If they are hostile to security researchers, this is a bad sign.)

If the service is free

- ☐ How does the vendor make money? Do they make money by selling access to—or products based on—your private data?
- ☐ Will they respond to customer service requests?
- ☐ How likely are they to invest in security infrastructure?

If participant data is involved

- ☐ Is the client data being stored and transmitted in accordance with the legally mandated provincial standards?
- ☐ How often do they re-audit that they are in compliance with these standards?
- ☐ Are the audit results publicly available?

DRAFT

Policy	Vendor Risk Assessment
--------	------------------------

Created date:	<DATE>
Applies to:	All Employees, Contractors and Volunteers
Approved by:	<PRIVACY OFFICER>

Purpose

The CIE will perform a vendor risk assessment to ensure that any existing or potential vendors comply with legal, regulatory, and operational standards, especially those related to data privacy, security, and patient care.

Protect Patient Privacy and Data Security

The CIE handles sensitive patient information protected under provincial legislation. Vendors who process, store, or transmit this data on behalf of the CIE pose a potential risk if they lack robust security measures.

- **Risk:** Unauthorized access, data breaches, or mishandling of protected health information (PHI).
- **Benefit:** Ensures vendors implement strong safeguards like encryption, access controls, and regular monitoring.

Ensure Regulatory Compliance

The CIE must ensure their vendors adhere to applicable laws and industry standards to avoid fines, legal action, and reputational damage.

- **Risk:** Non-compliance by a vendor can result in the CIE being held liable for violations.
- **Benefit:** A risk assessment helps identify gaps in vendors' compliance programs, ensuring alignment with federal and provincial legislations.

Mitigate Operational Risks

Vendors play a critical role in The CIE's operations, such as managing electronic health records (EHR), billing systems, or IT infrastructure. Assessing risks ensures business continuity and minimizes disruptions.

- **Risk:** Vendor failures, such as system outages, financial instability, or poor service quality, could impact patient care and clinic operations.
- **Benefit:** Identifying reliable vendors reduces the likelihood of operational disruptions.

Safeguard Reputation and Trust

Data breaches or vendor-related incidents can damage the the CIE's reputation and erode patient trust.

- **Risk:** Patients may lose confidence if their data is mishandled by a third-party vendor.
- **Benefit:** Demonstrating due diligence in vendor selection shows patients and regulators that the CIE prioritizes security and privacy.

Identify and Address Supply Chain Risks

Vendors may rely on their own subcontractors, creating a complex supply chain with additional risks. A vendor risk assessment can identify these dependencies and evaluate their potential impact on the CIE.

- **Risk:** Hidden vulnerabilities in the vendor's supply chain could lead to data leaks, legal issues, or service failures.
- **Benefit:** Greater visibility into supply chain risks allows the CIE to demand accountability and stronger controls.

Financial and Legal Protection

Unvetted vendors may expose The CIE to financial losses through lawsuits, fines, or contract disputes.

- **Risk:** Liability for data breaches or service failures caused by vendor negligence.
- **Benefit:** Ensures proper contractual protections, such as indemnity clauses, service agreements, and termination rights.

Support Informed Decision-Making

A vendor risk assessment provides a framework for evaluating vendors systematically based on their risk profile.

- **Risk:** Making decisions without assessing risks could lead to partnerships with unsuitable or high-risk vendors.
- **Benefit:** Enables the CIE to choose vendors who align with its security, compliance, and operational goals.

Key Areas of Vendor Risk Assessment

- **Data Protection and Privacy Practices:** Policies, encryption standards, access control measures, and auditing capabilities.
- **Regulatory Compliance:** Adherence to provincial privacy legislations.
- **Business Continuity and Disaster Recovery Plans:** Ability to maintain operations during disruptions.
- **Subcontractor Management:** Oversight of third-party vendors in the vendor's supply chain.
- **Financial Stability:** Assessment of the vendor's solvency and ability to deliver long-term services.

By performing a vendor risk assessment, the CIE can proactively manage risks, ensure high-quality patient care, and maintain compliance with legal and ethical obligations, ultimately protecting both the CIE and its participants.

Checklist

The CIE will complete the Vendor Assessment Checklist prior to entering an agreement with a vendor to ensure that they satisfactorily meet the criteria established in this policy.

DRAFT

Policy	Whistleblower
--------	---------------

Created date:	<DATE>
Applies to:	All Employees, Contractors and Volunteers
Approved by:	<PRIVACY OFFICER>

Purpose

The purpose of this Whistleblower Policy is to establish procedures for reporting and addressing actions or practices within the CIE that are believed to be illegal, unethical, or not in the best interests of the Organization, its mission, or its stakeholders.

Reporting Mechanism

Any individual who becomes aware of illegal, unethical, or non-compliant activities within the CIE is encouraged to report such concerns. Reports should be made in writing, detailing the nature of the concern and the evidence supporting it.

Reports can be submitted through any of the following channels:

- Directly to the Chair of the Steering Committee
- Through an email to a dedicated, confidential email address established for whistleblowing
- By mailing a written report to the CIE's physical address
- By other secure and confidential methods established by the CIE.

The CIE will ensure that all reports received are treated confidentially to the extent permitted by law.

Protection Against Retaliation

The CIE is committed to protecting individuals who report concerns in good faith from any form of retaliation, harassment, or adverse actions.

Anyone who feels they have suffered retaliation for reporting concerns should immediately report the retaliation to the Chair of the Steering Committee or to the Executive Director.

Retaliation against a whistleblower is a violation of this policy and will be subject to disciplinary action.

Investigation Process

The Chair of the Steering Committee shall appoint an independent investigator or committee to conduct an investigation into the reported concern.

The investigation shall be conducted confidentially and impartially. The investigator(s) shall have no conflict of interest related to the matter under investigation.

The investigator(s) will report their findings to the Chair of the Steering Committee, who will determine appropriate action based on the investigation's results.

Communication of Findings

Following the investigation, the Chair of the Steering Committee will provide the whistleblower with a summary of the findings and any corrective actions taken or proposed.

If the individual reporting the concern remains unsatisfied with the resolution, they may report the matter to external authorities as permitted by law.

Records Retention

The CIE will maintain records of all whistleblower reports, investigations, and actions taken, as required by law.

Non-Retaliation Assurance

All members of the Steering Committee and volunteers are prohibited from retaliating against individuals who report concerns in good faith.

Any violation of this non-retaliation assurance will be subject to disciplinary action.