



Protection of Electronic Data Policy

Policy Number: D-02

Version: 1

Approved by the Board on: **March 17, 2025**

Responsible Person: Director, Operations

Scheduled Review Date: January 1, 2026

Revision Date: March 10, 2025

Purpose

The purpose of this policy is to ensure the protection of electronic data within NCIME, safeguarding it against unauthorized access, disclosure, alteration, and destruction. This policy outlines the responsibilities and procedures for managing and securing electronic data.

Scope

This policy applies to all employees, contractors, and third-party service providers who handle electronic data on behalf of NCIME.

Definitions

- **Privacy Officer (PO):** The individual responsible for overseeing the implementation and maintenance of data protection policies.
- **IT & Database Manager:** The individual responsible for managing technical safeguards and ensuring the security of NCIME's IT infrastructure.
- **Personal Information:** Any information that can identify an individual, such as name, address, email, and phone number.
- **Encryption:** The process of converting data into a code to prevent unauthorized access.
- **Multi-Factor Authentication (MFA):** A security system that requires more than one method of authentication to verify the user's identity.

Governance and Accountability

- **Privacy Officer (PO):** The PO is responsible for overseeing the implementation and maintenance of this policy, ensuring compliance with relevant laws and regulations.
- **IT & Database Manager:** The IT & Database Manager manages technical safeguards and ensures the security of NCIME's IT infrastructure.



- **Employees and Contractors:** All employees and contractors must adhere to this policy and report any security incidents to the PO.

Data Collection and Use

- **Minimization:** Collect only the data necessary for the specified purpose.
- **Transparency:** Inform individuals about the purpose of data collection and how their data will be used.
- **Consent:** Obtain explicit consent from individuals before collecting their data, unless otherwise permitted by law.

Data Access and Use

- **Role-Based Access Control (RBAC):** Access to electronic data is granted based on the individual's role and responsibilities within NCIME.
- **Least Privilege Principle:** Users are granted the minimum level of access necessary to perform their job functions.
- **Authentication:** Implement strong authentication mechanisms, including multi-factor authentication (MFA), to verify user identities.

Data Security Measures

- **Encryption:** Encrypt sensitive data both at rest and in transit using industry-standard encryption protocols.
- **Secure Storage:** Store electronic data in secure environments with appropriate physical and technical safeguards- Sharepoint, NCIME Database.
- **Regular Audits:** Conduct regular security audits and vulnerability assessments to identify and mitigate risks.

Data Sharing and Disclosure

- **Third-Party Agreements:** Ensure that third-party service providers comply with NCIME's data protection standards through contractual agreements.
- **Data Sharing:** Share data only with authorized parties and for legitimate purposes, ensuring that data is adequately protected during transfer.

Data Retention and Disposal

- **Retention Periods:** Retain electronic data only for as long as necessary to fulfill the purpose for which it was collected.



- **Secure Disposal:** Dispose of electronic data securely when it is no longer needed, using methods such as shredding or secure deletion.

Incident Response

- **Reporting:** Report any data breaches or security incidents to the PO immediately.
- **Containment:** Take immediate steps to contain and mitigate the impact of the breach.
- **Notification:** Notify affected individuals and relevant authorities as required by law.

Training and Awareness

- **Employee Training:** Provide regular training to employees on data protection and security best practices.
- **Awareness Programs:** Conduct awareness programs to promote a culture of data protection within NCIME.

Compliance and Review

- **Compliance Monitoring:** Regularly monitor compliance with this policy and relevant data protection laws.
- **Policy Review:** Review and update this policy annually or as needed to ensure its effectiveness.

References

- **Personal Information Protection and Electronic Documents Act (PIPEDA)**
- **ISO/IEC 27001: Information Security Management**

Keywords

- Data Protection
- Electronic Data
- Security
- Encryption
- Multi-Factor Authentication
- Data Retention
- Data Disposal
- Incident Response

NCIME

THE NATIONAL CIRCLE FOR
INDIGENOUS MEDICAL EDUCATION



CNFMSA

LE CERCLE NATIONAL POUR
LA FORMATION MÉDICALE EN SANTÉ AUTOCHTONE