Data Protection & Encryption Policy

OpenMRS Canadian Clinic
Version 1.0 | Effective Date: April 2026
Policy Owner: Clinic Manager

Purpose

To establish requirements for protecting the confidentiality, integrity, and availability of patient data through appropriate encryption and data handling practices in compliance with PHIPA and PIPEDA.

Scope

This policy applies to all patient data, systems, and devices used to store, process, or transmit information in the OpenMRS environment.

Policy Statements

- All patient data must be protected at rest and in transit using strong encryption.
- Data transmitted over networks (including the web interface) must use TLS 1.3 or higher.
- The PostgreSQL database must have encryption enabled for data at rest.
- Removable media and backups containing patient data must be encrypted.
- Encryption keys must be securely managed and rotated regularly.
- Data minimization principles must be followed – only connect and retain the minimum data necessary.

Technical Requirements

- Encryption algorithms must meet or exceed current industry standards (e.g., AES-256)
- Regular vulnerability scans and penetration testing will be conducted to verify encryption effectiveness.
- Encryption settings will be verified quarterly.

Responsibilities

- **IT Lead:** Implement and maintain encryption controls and key management.
- **Clinic Manager:** Ensure staff training on data protection and policy compliance.
- **All Users:** Handle patient data securely and report any suspected loss or compromise immediately.

Enforcement

Violations of this policy may result in disciplinary action and regulatory reporting where required.

Review

This policy will be reviewed annually or following any significant security incident or technological change.