Incident Response Policy

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

Purpose

To establish a clear, effective process for detecting, responding to, and recovering from security incidents involving patient data or OpenMRS systems, while meeting PHIPA breach notification obligations.

Scope

This policy applies to any suspected or confirmed security incident, data breach, unauthorized access, or system compromise.

Policy Statements

- All suspected incidents must be reported to the Clinic Manager within 1 hour.
- The clinic will comply with PHIPA requirements for notifying affected individuals and the Information and Privacy Commissioner of Ontario.
- A designated incident response team will be activated for significant events.
- All incidents will be thoroughly documented, including containment, eradication, recovery, and post-incident lessons learned.

Incident Response Process

1. Identification and Reporting
2. Containment
3. Eradication
4. Recovery
5. Post-Incident Review and Lessons Learned

Annual Testing

A tabletop exercise simulating a breach scenario will be conducted at least annually with relevant staff.

Review

This policy will be reviewed annually or following any significant organizational or system change.