Privacy and Confidentiality Policy

This document is prepared by www.pharmasist.ca

Patient information and pharmacy operational information must only be accessed, used, discussed, or disclosed when authorized and necessary.

1. Objective and Scope

This policy establishes strict guidelines for maintaining privacy and confidentiality, with a focus on safeguarding patient information and pharmacy operations. It applies to all pharmacists, pharmacy technicians, support staff, management, students, volunteers, contractors, and any person with access to pharmacy information.

Handling Patient Information

- Access patient information only when required for job duties.
- Use information only for patient care, pharmacy operations, or legal requirements.
- Do not discuss patient information in public areas.
- Do not disclose information to unauthorized persons.
- Use the minimum necessary information when sharing is required.

Confidentiality Agreement

- All employees must sign a confidentiality agreement upon hiring.
- The agreement confirms the employee's duty to protect patient privacy.
- Confidentiality obligations continue after employment ends.
- Breaches may result in disciplinary action.

2. Data Security

- Electronic patient records must be stored in secure, password-protected systems.
- Use encryption where available and appropriate.
- Passwords must not be shared.
- Workstations must be locked when unattended.
- Physical documents containing patient information must be stored in locked cabinets or restricted areas.
- Access must be limited to authorized personnel only.

Access Control

- Access to confidential data is limited to staff who need it for their role.
- Patient record access may be logged.
- Periodic audits may be conducted.
- Unnecessary browsing of patient profiles is prohibited.
- Access privileges must be updated when roles change.

Disclosure Protocol

- Do not disclose patient information without consent unless required by law.
- Confirm identity before sharing information.
- Share only the minimum necessary information.
- Document disclosure when required.
- Use secure communication methods.

3. Patient Consent

- Obtain verbal or written consent before using patient health information for purposes other than direct care, unless legally permitted.
- Patients must be informed of their rights regarding personal health information.
- Consent discussions should be documented when appropriate.
- Respect patient restrictions and preferences where legally and operationally possible.

Privacy Breach Reporting

- Report suspected privacy breaches immediately to the designated privacy officer or manager.
- Secure affected records or systems immediately.
- Document what happened, when it happened, and who was involved.
- Investigate breaches promptly.
- Implement corrective measures.

Examples of Breaches

- Patient profile opened without work-related reason.
- Prescription left visible to the public.
- Patient information discussed where others can hear.
- Information sent to the wrong fax, email, or person.
- Lost document containing personal health information.

4. Employee Training

- Privacy and confidentiality training is mandatory for all employees.
- New employees must complete training during orientation.
- Annual refresher training must be completed.
- Training records must be retained.
- Staff must be trained on secure communication, breach reporting, and proper handling of patient information.

5. Compliance and Auditing

- Regular audits may be conducted to confirm compliance.
- Audit findings must be reviewed by management or the designated privacy officer.
- Corrective action must be taken when gaps are identified.
- Non-compliance may result in disciplinary action, up to and including termination.

6. Review and Update

This policy will be reviewed annually and updated as necessary to reflect changes in legal requirements, privacy standards, pharmacy operations, technology, and best practices.