Ajax Women's Health Clinic

PATIENT PRIVACY POLICY

Compliant with the Personal Health Information Protection Act (PHIPA), S.O. 2004, c. 3, Sched. A

1. Policy

Ajax Women's Health Clinic is committed to protecting the privacy of our patients and the confidentiality of their personal health information (PHI). As a health information custodian under the Personal Health Information Protection Act (PHIPA), we are legally obligated to comply with all requirements of PHIPA and its regulations, and we take that obligation seriously.

This Privacy Policy explains how we collect, use, share, and safeguard personal health information, and describes the rights of a patient. We collect and use PHI for the following primary purposes:

- To assess, diagnose, and treat health conditions and to provide patients with ongoing health care.
- To coordinate patient care with other health care providers involved in treatment.
- To fulfill our legal and regulatory obligations, including reporting requirements under applicable legislation.
- To manage billing and obtain payment for insured and uninsured health care services.
- To support quality improvement, error management, and risk management activities within the Practice.
- To conduct or support health research or health system planning, evaluation, or analysis, subject to applicable conditions.

We collect, use, and disclose only the minimum amount of PHI necessary to fulfill the purposes described in this Policy.

2. Collection of Personal Health Information

We may collect personal health information in the following ways:

- Directly from the patient, through written intake and registration forms, questionnaires, or consent forms.
- Verbally during consultations, telephone conversations, or appointments.
- Through secure electronic health record (EHR) systems or patient portals.
- From other health care providers who are involved in a patient's care, such as specialists, hospitals, or other practitioners to whom a patient has been referred.
- From health care facilities, including hospitals, clinics, and long-term care homes.

We may receive PHI from the following sources:

- Medical laboratories and diagnostic imaging clinics.
- Pharmacies and pharmacists.
- Other health care providers and specialists involved in a patient's care.
- Substitute decision-makers legally authorized to act on the patient's behalf.

- Ontario Health (formerly eHealth Ontario) and related health information networks, where applicable.
- The Ministry of Health and Long-Term Care, for administrative and billing purposes.

3. Use of Personal Health Information

We use a patient's personal health information for the following purposes:

Primary Health Care Purposes

- To assess, diagnose, and treat a patient's health conditions.
- To monitor ongoing health status and manage chronic conditions.
- To communicate with the patient regarding appointment scheduling, follow-up care, test results, and treatment recommendations.
- To refer the patient to specialists or other health care providers for diagnostic testing or specialized treatment.

Administrative and Billing Purposes

- To process and submit claims to the Ontario Health Insurance Plan (OHIP) or other applicable insurers for insured services.
- To invoice and obtain payment for uninsured or additional services provided on a fee-for-service basis.
- To maintain accurate and up-to-date health records as required by law.

Quality Improvement and Risk Management

- To identify and address errors or near-miss events and to improve patient safety.
- To conduct internal audits and quality assurance reviews.
- To support accreditation activities where applicable.

Other Permitted Purposes

- To comply with legal obligations, including mandatory reporting requirements (e.g., communicable diseases, child protection concerns).
- To support health research or health system planning and evaluation, subject to the conditions set out in PHIPA and applicable guidelines.

4. Disclosure of Personal Health Information

We may share personal health information with others in the following circumstances:

Circle of Care

We may share PHI with other health care providers involved in the provision of health care to a patient, including specialists, hospitals, pharmacies, laboratories, and other treating clinicians. This sharing occurs on the basis of a patient's implied consent, provided they have not withdrawn or restricted consent.

Billing and Payment

We are required to disclose certain PHI to the Ministry of Health and Long-Term Care, OHIP, or other applicable payers for the purposes of billing for and obtaining payment for health care services rendered, without requiring express consent.

Legal and Regulatory Obligations

- To public health authorities, as required by the Health Protection and Promotion Act or other applicable legislation (e.g., reporting of communicable diseases).
- To regulatory bodies or law enforcement agencies, as required or authorized by law.
- To child protection authorities, as required under the Child, Youth and Family Services Act.
- In circumstances where disclosure is necessary to eliminate or significantly reduce a serious and imminent risk of bodily harm to the patient or another person.

Research and Health System Planning

We may disclose PHI for health research, planning, evaluation, or analysis purposes to prescribed entities, research ethics board-approved researchers, or public health agencies, subject to the conditions set out in PHIPA and only where required privacy safeguards are in place.

With Express Consent

In circumstances not described above, for example, disclosure to a lawyer, insurance company, or employer, we will only share a patient's PHI with their express, written consent.

5. Protection of Personal Health Information

We implement reasonable physical, administrative, and technical safeguards to protect PHI against unauthorized access, collection, use, disclosure, copying, modification, disposal, or destruction.

Storage

- PHI is stored in secure electronic health record (EHR) systems protected by access controls, encryption, and audit logging, and/or in locked physical filing systems accessible only to authorized personnel.
- Electronic records are maintained on secured servers with role-based access controls and regular security updates.

Physical Safeguards

- Paper records are stored in locked filing cabinets within secure, access-controlled areas of the Practice.
- Workstations and devices are secured with password protection and screen-lock features.
- Visitors to clinical areas are supervised, and access to records storage areas is restricted to authorized staff.

Administrative Safeguards

- All staff and contractors with access to PHI receive privacy and security training upon hire and on an ongoing basis.
- Access to PHI is granted on a need-to-know basis appropriate to each individual's role.

- Staff are required to sign confidentiality agreements as a condition of employment or engagement.

Technical Safeguards

- All electronic transmissions of PHI are encrypted using industry-standard protocols.
- Multi-factor authentication is used where applicable to protect access to electronic systems.
- Regular data backups are performed, and backup media is stored securely.

Retention and Destruction

We retain PHI for the minimum period required by law and our professional obligations. Under the PHIPA regulation and applicable professional standards, patient health records are generally retained for at least 10 years from the date of the last entry, or, in the case of a minor, until the patient turns 28 years of age (or such other period as required by law).

Upon expiry of the applicable retention period, PHI will be permanently and securely destroyed in a manner that renders it unreadable and unrecoverable, for example, cross-cut shredding of paper records and secure electronic deletion or physical destruction of digital media.

6. Consent

Implied Consent

In most circumstances, we rely on a patient's implied consent to collect, use, and disclose their PHI for the purpose of providing health care. Implied consent exists where a patient voluntarily seeks health care from the Practice and it is reasonable to conclude that they consent to the collection, use, and disclosure of their PHI within their circle of care for that purpose.

Express Consent

Express consent, whether written or verbal, and clearly communicated, is required in the following circumstances:

- Disclosure of PHI to persons who are not health care providers and are not within the patient's circle of care (e.g., lawyers, insurers, employers).
- Collection, use, or disclosure of PHI for marketing purposes or market research, except as may be excluded by the PHIPA regulation (e.g., communications by insured-service practitioners about additional uninsured services offered by the Practice).
- Use or disclosure of PHI for any purpose not reasonably related to the provision of health care, except as otherwise permitted by law.

Withdrawal of Consent and Consent Directives

Patients have the right to withhold or withdraw consent to the collection, use, or disclosure of their PHI, or to place restrictions on who may access your record. These restrictions are called consent directives and may be placed by our Clinic Manager when submitted in writing. Please be aware that withdrawing consent may affect our ability to provide care, and that certain disclosures required by law (such as public health reporting or billing to OHIP) may proceed without a patient’s consent.

Substitute Decision-Makers

Where a patient lacks the capacity to consent to the collection, use, or disclosure of their PHI, a substitute decision-maker authorized under PHIPA may make decisions on their behalf. Our Practice will follow the applicable requirements governing who may act as a substitute decision-maker and under what circumstances. For further information, please refer to the Information and Privacy Commissioner of Ontario's Guide to the Personal Health Information Protection Act.

Permitted or Required Disclosures Without Consent

In certain circumstances, PHIPA permits or requires the collection, use, or disclosure of PHI without the patient's consent, including but not limited to:

- Billing and payment for health care services.
- Mandatory reporting obligations (communicable disease, gunshot wounds, child protection).
- Health planning, evaluation, or analysis by prescribed entities.
- Disclosure to reduce or eliminate a significant risk of serious bodily harm.
- Compliance with a court order or other legal process.

7. Responding to Privacy Inquiries, Requests, and Breaches

Patient Rights

All patients have the right to:

- Request access to their personal health information held by this Practice.
- Request corrections or amendments to their PHI if it is believed to be inaccurate or incomplete.
- Withdraw or restrict consent for the collection, use, or disclosure of their PHI.
- File a complaint with the Practice's Privacy Officer or with the Information and Privacy Commissioner of Ontario (IPC).

How to Submit a Request or Complaint

To exercise any of the rights above, or to submit a privacy concern or complaint, please contact our Privacy Officer:

Dr. Hossai Furmli, MD FRCPC

Ajax Women's Health Clinic

Unit 5 - 279 Kingston Road East, Ajax, ON L1Z 0K5

Phone: 416-350-1944

Email: info@ajaxwomenshealth.ca (encrypted communication preferred)

We will acknowledge the request within two (2) business days and will endeavor to respond fully within thirty (30) days of receipt, as required by PHIPA. If additional time is required, we will notify you in writing with an explanation.

Privacy Incidents and Breaches

In the event that personal health information is lost, stolen, accessed, used, or disclosed without authorization, we will:

- Act promptly to contain the breach and prevent further unauthorized access or disclosure.

- Investigate the circumstances of the breach and identify all affected individuals.
- Notify affected individuals at the first reasonable opportunity, providing sufficient information about the breach and the steps taken in response.
- Notify the Information and Privacy Commissioner of Ontario (IPC) where required by law or where appropriate given the severity of the breach.
- Document the breach and implement corrective measures to reduce the risk of recurrence.

8. Monitoring and Enforcement

We are committed to ensuring ongoing compliance with this Privacy Policy and with PHIPA. To that end:

- All employees, contractors, and agents with access to PHI are required to read, understand, and comply with this Privacy Policy as a condition of their employment or engagement.
- Privacy and security training is provided to all staff upon hire and on a regular ongoing basis.
- Compliance with this Policy is monitored through periodic internal privacy and security audits, conducted at least annually or as circumstances require.
- Access logs for electronic health record systems are reviewed regularly to detect unauthorized access or anomalous activity.
- Non-compliance with this Policy, PHIPA, or applicable privacy obligations may result in disciplinary action up to and including termination of employment or engagement and may also result in regulatory or legal proceedings.

Review and Revision: This Privacy Policy will be reviewed annually and updated as needed to reflect

- Changes in applicable law or regulatory guidance, including IPC guidance and PHIPA amendments.
- Recommendations arising from privacy impact assessments or privacy and security audits.
- Changes to our information systems, technology, or practices.
- Identified privacy incidents, breaches, or near-miss events.