

PRIVACY STATEMENT AND WRITTEN DESCRIPTION OF INFORMATION PRACTICES

Personal Health Information Protection Act, 2004 • Ontario Regulation 329/04

Effective Date: October 14, 2026 Last Updated: October 2026

At Flemingdon Health Centre (“FHC”, “we”, “our”, or “us”), we are committed to protecting the privacy, confidentiality, integrity, and security of your personal health information (“Your Information”).

This Written Statement explains how FHC collects, uses, discloses, stores, protects, retains, and manages Your Information in accordance with the Personal Health Information Protection Act, 2004 (“Ontario’s Privacy Legislation”), Ontario Regulation 329/04, and other applicable laws and professional obligations.

This statement describes FHC’s role as a Health Information Custodian (“HIC”); FHC’s role as a Health Information Network Provider (“HINP”); how FHC authorizes and manages internal and external Agents; how electronic medical record systems and authorized technologies, including approved artificial intelligence tools, are used; how cameras are used; and the safeguards FHC maintains to protect Your Information.

1. Our Role as a Health Information Custodian

FHC is a Health Information Custodian under Ontario’s Privacy Legislation. As a HIC, FHC is legally responsible for protecting the privacy and security of Your Information.

FHC remains accountable for Your Information as it is handled by FHC’s employees, physicians, students, volunteers, contractors, consultants, service providers, and other individuals or organizations acting on its behalf (“Agents”).

FHC authorizes Agents to access or handle Your Information only where:

- the activity is authorized by Ontario’s Privacy Legislation;
- the activity is necessary for authorized health care (including the circle of care), operational, administrative, or support purposes;
- written agreements and confidentiality obligations are in place where required; and
- the Agent has completed mandatory privacy and security training.

Access to Your Information is limited to the minimum amount reasonably necessary to perform assigned duties. FHC requires all Agents to comply with Ontario’s Privacy Legislation, FHC privacy and security policies, confidentiality obligations, and applicable safeguards.

2. Collection of Personal Health Information

FHC collects Your Information directly from you or from a person legally authorized to act on your behalf.

We may collect information such as your:

- name, date of birth, address, contact information, and health card number;
- demographic and identification information;
- medical, mental health, social, and family health history;
- records of visits, assessments, diagnoses, medications, treatments, and care plans;
- laboratory, diagnostic imaging, and consultation reports;
- referrals and communications with other health care providers;
- appointment, scheduling, and billing information;
- images or video captured for authorized teaching purposes or by security cameras, where applicable; and
- other information reasonably necessary to provide health care and related services.

In some circumstances, FHC may collect Your Information from hospitals, physicians, pharmacies, laboratories, community agencies, caregivers, substitute decision-makers, or other health care providers where you have consented; Ontario's Privacy Legislation permits or requires the collection without consent; or the collection is necessary for the provision of health care or a related authorized purpose.

FHC limits collection to the minimum amount reasonably necessary for authorized purposes.

3. Uses and Disclosures of Personal Health Information

3.1 Authorized purposes

FHC collects, uses, and discloses Your Information only as permitted or required by Ontario's Privacy Legislation and other applicable laws. Depending on the circumstances and legal authority, we may collect, use, or disclose Your Information:

- to provide, coordinate, support, and improve your health care and related services;
- to communicate with other health care providers involved in your care (circle of care);
- to support integrated and collaborative care with authorized participating health care organizations and providers;
- to verify your identity and eligibility for services;
- to communicate with you about your care, appointments, follow-up, treatment options, community resources, health education, programs, services, events, and other information that may support your health and well-being;
- to obtain payment or reimbursement for services, including from OHIP, WSIB, private insurers, or other authorized payers;
- to plan, administer, manage, evaluate, monitor, and improve our programs, services, operations, and quality of care;
- to conduct quality improvement, risk management, client safety, utilization management, and patient experience activities;
- to conduct audits, investigations, monitoring, and compliance activities relating to privacy, security, and professional obligations;
- to educate and train students, staff, residents, and other authorized health professionals;
- to conduct research, where authorized by law and approved through appropriate research ethics and privacy processes;
- for statistical and reporting obligations supporting care, including sharing with provincial health information systems (such as those operated or funded by Ontario Health) where authorized by law;
- to send newsletters, updates, and information about FHC programs, services, initiatives, events, community activities, or health promotion opportunities, where permitted by law;
- to conduct fundraising activities in accordance with Ontario's Privacy Legislation and other applicable laws (you may withdraw consent to fundraising communications at any time);
- to comply with legal, regulatory, accreditation, professional, public health, and reporting obligations; and
- to fulfill any other purpose permitted or required by law.

FHC does not sell Your Information. Your Information is accessed or used only on a need-to-know basis for authorized purposes. FHC prohibits unauthorized access, including accessing records out of curiosity or for personal reasons.

3.2 Consent, withdrawal, and lockbox (consent directive)

We may rely on implied consent to collect, use, and disclose Your Information for the purpose of providing health care or assisting in providing you with health care.

Where required by law, FHC will obtain your express consent before collecting, using, or disclosing Your Information, including for non-health care purposes and before first use of an authorized AI Scribe.

You may withdraw your consent for certain uses or disclosures, subject to legal and operational limitations.

Ontario's Privacy Legislation grants you the right to request a consent directive, also known as a "lockbox," to withdraw or withhold consent for the collection, use, or disclosure of Your Information for health care purposes. You may implement a consent directive to restrict access by one or more FHC staff, or to restrict disclosure to external health care providers (such as your family doctor or another health care facility).

Risks you should consider before requesting a consent directive:

- Your clinician may not have enough current or accurate information to give you the best possible care.
- Your clinician may not have the information required to safely provide care or services and, in some cases, may be unable to offer treatment.

3.3 When FHC may collect, use, or disclose without consent

There are times when FHC can or must collect, use, or disclose Information about you without your consent — including where a consent directive is in place. Examples include:

- where FHC has reasonable grounds to believe that accessing or sharing Your Information is necessary to eliminate or reduce a significant risk of serious bodily harm to you or others (for example, a medical emergency);
- where Your Information is reasonably necessary to examine, assess, observe, or detain you in accordance with the Mental Health Act, or to comply with the Criminal Code or a court order; and
- where disclosure is required to fulfill a mandatory reporting duty under another law — for example, a report to a children's aid society under the Child, Youth and Family Services Act, 2017 if a child is believed to be in need of protection, or to the Ontario Ministry of Transportation under the Highway Traffic Act if a health condition may make you unfit to drive.

You may discuss privacy concerns and consent directives with FHC staff or the Privacy Officer.

3.4 Aggregated and de-identified information

We may modify or aggregate (de-identify) Your Information so that it cannot reasonably be associated with you, for the purposes of protecting privacy and conducting research or analytics to improve services.

De-identified or aggregate information may be shared with government entities, research entities, and health care organizations for purposes such as measuring performance, improving health care delivery in Ontario, improving FHC operations, research or statistics, or developing products or services.

4. Electronic Medical Record Systems

FHC supports and manages an electronic medical record ("EMR") environment. Authorized health care providers involved in your care may use the EMR to securely access and manage Your Information, including demographics, clinical documentation and assessments, medications and prescriptions, laboratory and diagnostic information, referrals and consultations, treatment plans, and other information reasonably necessary to support care.

FHC is responsible for supporting the secure operation, management, oversight, monitoring, and governance of the EMR environment as required under Ontario's Privacy Legislation and applicable agreements.

5. Use of Artificial Intelligence (AI) Tools

FHC may use approved artificial intelligence tools to support health care delivery, clinical documentation, operational efficiency, administrative activities, and service improvement. FHC recognizes that AI tools may create additional privacy, confidentiality, security, and accuracy risks and is committed to ensuring that all AI use complies with Ontario's Privacy Legislation, FHC policies, contractual obligations, and applicable professional standards.

5.1 Approved AI tools

Approved AI tools that may currently be used by FHC include:

- authorized AI Scribes used to support clinical documentation during or after patient encounters; and
- AI such as Microsoft Copilot for Microsoft 365, for approved administrative and productivity purposes only.

5.2 Restrictions

FHC must obtain your express consent before we use an AI Scribe for the first time, and we must record that consent in your health record.

FHC prohibits the use of public or third-party generative AI tools for processing, storing, transmitting, summarizing, analyzing, or generating content containing identifiable personal health information unless the AI solution has been formally approved by FHC and is compliant with Ontario's Privacy Legislation and approved safeguards.

Only AI solutions formally reviewed and approved by FHC may be used with Your Information. Approved AI tools are treated as external Agents of FHC and are subject to contractual, privacy, security, confidentiality, audit, and oversight requirements.

5.3 Your right to refuse or opt out of AI use

You may request that AI tools not be used during your care encounter. If you prefer not to have AI used during your appointment or interaction, inform your provider or any FHC staff member. Refusing or opting out of AI use will not negatively affect the care or services you receive from FHC.

In addition to obtaining express consent, FHC may provide verbal notification, signage, written notices, or other communications where AI tools may be used. You may withdraw consent to the collection, use, or disclosure of Your Information through the AI Scribe and continue to receive the same or a similar level of care.

5.4 Human oversight

All AI-generated or AI-assisted clinical documentation and outputs are subject to human review and oversight for accuracy. Qualified health care providers remain responsible for reviewing, verifying, editing, approving, and finalizing clinical documentation and care decisions. AI tools do not replace professional judgment or clinical decision-making.

6. Cameras and Video Recording

6.1 Teaching and supervised learning cameras

Designated clinical rooms are equipped with cameras used only for teaching and supervised learning. These cameras provide a live feed to the supervising staff responsible for the teaching or supervision activity. They do not record, photograph, store, or share the encounter.

A teaching camera is turned on only after you give permission. Before it is used, you will be told that FHC is a teaching clinic; that the camera is used only for teaching and supervised learning by live feed; that viewing is limited to the supervising staff unless you give permission for someone else to observe; and that you may refuse, or ask that the camera be turned off, at any time.

Your decision will not affect the care or services you receive. If you lack decision-making capacity, permission is obtained from your substitute decision-maker. Signs are posted in rooms where a teaching camera is present.

6.2 Security cameras (CCTV)

FHC also operates security cameras that may record video in designated areas of its premises, such as entrances, waiting areas, hallways, and other common spaces. Security cameras are used to protect the safety and security of clients, staff, visitors, and property, and to support investigation of safety, security, or privacy incidents. FHC's security cameras record video only. Recordings may include your image. Signs are posted to notify you that security cameras are in use.

7. How We Protect Personal Health Information

We use a combination of administrative, technical, physical, contractual, and organizational safeguards to protect Your Information against theft, loss, unauthorized access, use, disclosure, copying, modification, disposal, or destruction. Safeguards include:

- role-based access controls and least-privilege access;
- formal access approval and revocation procedures;
- unique user accounts and authentication controls;
- strong password requirements and multi-factor authentication where implemented;
- encryption of information in transit and, where appropriate, at rest;
- secure remote access methods;
- electronic audit logging and system monitoring;
- cybersecurity protections including anti-malware software, firewalls, endpoint protections, threat monitoring, vulnerability assessments, and penetration tests;
- periodic audits and investigations relating to access and use of personal health information;
- mandatory privacy and security training;
- confidentiality agreements and non-disclosure obligations;
- secure destruction of records and media;
- locked cabinets and restricted physical access for paper records and secure workspaces;
- privacy impact assessments and threat risk assessments;
- vendor and third-party oversight processes; and
- business continuity and disaster recovery processes.

FHC regularly reviews and updates safeguards to address evolving risks, technologies, operational requirements, and legal obligations.

8. Authorized Users, Agents, and Access Controls

Access to Your Information is restricted to authorized individuals who require access to perform health care, operational, administrative, educational, or support functions.

Before being granted access to Your Information or FHC systems, authorized users must complete mandatory privacy and security training; sign confidentiality agreements; comply with FHC policies and procedures; and receive appropriate authorization and approval.

FHC may suspend, restrict, or terminate access where training requirements are not completed; unauthorized access or misuse is suspected; an employment, affiliation, or contractual relationship ends; or access is no longer required.

FHC maintains audit logs and may review user activity, investigate suspicious access, and conduct compliance reviews.

9. Data Storage, Retention, and Destruction

FHC retains Your Information only for as long as necessary to fulfill authorized purposes and meet legal, professional, operational, and regulatory requirements.

Unless expressly authorized otherwise, Your Information is stored and processed within Canada.

When Your Information is no longer required, FHC securely destroys or permanently de-identifies it using approved methods designed to prevent reconstruction, unauthorized access, or recovery. FHC requires Agents, service providers, and third

parties handling personal health information on its behalf to comply with equivalent retention, return, destruction, and certification requirements.

10. Our Role as a Health Information Network Provider (HINP)

Under Ontario's Privacy Legislation and Ontario Regulation 329/04, organizations that provide electronic systems or services enabling health care providers to share personal health information electronically may be Health Information Network Providers.

FHC acts as a HINP in relation to certain electronic systems and services that support participating Health Information Custodians, such as health care organizations and authorized providers, to share personal health information with one another. As a HINP, FHC supports secure electronic access, exchange, processing, transmission, storage, and management of personal health information between authorized HICs.

Participating health care organizations may include, but are not limited to:

- North York Toronto Health Partners
- East Toronto Health Partners
- Michael Garron Hospital
- Baycrest Hospital
- Better Living Health and Community Services
- VHA Home HealthCare

In hosting the system, FHC protects Your Information by:

- entering into written agreements with each HIC concerning the services provided;
- using the personal health information of a HIC only to support the purposes and provide the specific services identified in the agreement;
- not using the personal health information of a HIC for FHC's own purposes;
- entering into written agreements with authorized Agents governing the handling of any personal health information;
- limiting access to individuals who need to know in order to provide services to the HIC;
- not disclosing the personal health information of a HIC unless authorized by that HIC or permitted or required by law;
- not altering personal health information managed on behalf of a HIC unless the alteration is described in the written agreement as an authorized use, or has been requested in writing by the HIC;
- conducting scheduled privacy audit activities to determine whether FHC staff comply with FHC's privacy obligations as a service provider;
- providing HICs with the results of privacy audits on request;
- conducting privacy audit activities at the request of a HIC to support management or investigation of a privacy incident or complaint;
- supporting HICs in responding to privacy complaints that relate to the services FHC provides;
- notifying participating HICs of any privacy breaches detected; and
- maintaining appropriate logging and monitoring of personal health information, to be made available to participating HICs on request.

FHC also maintains policies and procedures respecting privacy incidents; retention and storage of records; storage of personal health information; information security; access controls; encryption; privacy and security training; and logging, monitoring, and auditing.

11. Privacy Incidents and Breach Management

FHC requires all employees, Agents, contractors, service providers, and authorized users to immediately report suspected or confirmed privacy or security incidents involving Your Information. Examples include unauthorized access, use, or disclosure; lost or stolen devices or records; phishing or cybersecurity incidents; improper transmission of Your Information; or other events affecting confidentiality, integrity, or availability.

FHC investigates incidents and takes appropriate containment, mitigation, remediation, notification, and corrective action as required by law and organizational policy. Where required by Ontario's Privacy Legislation, FHC will notify affected individuals, participating health care providers, the Information and Privacy Commissioner of Ontario, or other parties.

12. Your Rights

Subject to limited legal exceptions, you have the right to:

- request access to a copy of Your Information;
- request correction of inaccurate or incomplete health records;
- withdraw or withhold consent for certain collections, uses, or disclosures;
- expressly instruct that Your Information not be used or disclosed for health care purposes without your consent (consent directive / lockbox);
- request information about FHC's privacy practices; and
- make a complaint regarding FHC's handling of Your Information to the Information and Privacy Commissioner of Ontario.

Requests relating to access, correction, or privacy concerns may be directed to FHC's Privacy Office.

13. How to Contact Us

If you have questions about this Privacy Statement or FHC's privacy and security practices, or if you wish to raise a privacy concern or complaint, please contact:

Samyuktha Pandalangat, Privacy Officer

Flemingdon Health Centre

10 Gateway Boulevard

Toronto, Ontario M3C 3A1

Telephone: 416-429-4991 ext. 254

Email: privacy@fhc-chc.com

14. Information and Privacy Commissioner of Ontario

You have the right to make a complaint to the Information and Privacy Commissioner of Ontario if you believe your privacy rights have been violated.

Information and Privacy Commissioner of Ontario

2 Bloor Street East, Suite 1400

Toronto, Ontario M4W 1A8

Telephone: 416-326-3333

Toll free: 1-800-387-0073