Health Report Manager (HRM®)

Privacy Policy

Last Updated: July 2, 2026

Table of Contents

1. Governing the Collection, Use and Disclosure of Personal Information (PI) and Personal Health Information (PHI)

In accordance with the *Personal Health Information Protection Act* (PHIPA), the safeguarding of an individual's privacy is critical to OntarioMD's role as a Health Information Network Provider (HINP) for the Health Report Manager (HRM®) application.

A HINP is defined as, "a person who provides services to two or more health information custodians where the services are provided primarily to custodians to enable the custodians to use electronic means to disclose personal health information to one another, whether or not the person is an agent of any of the custodians." Ontario Reg. 329/04, s. 6 (2).

2. Description of Services

HRM® is an OntarioMD managed digital health solution that securely delivers medical record reports from participating hospitals and specialty clinics (sending facilities) to patient charts within clinicians' Electronic Medical Records (EMRs) (receiving facilities). This solution replaces the process of paper copies and faxes being sent to the clinician's office and either integrating them into the EMR manually or managing them outside of the EMR.

With HRM, Discharge Summaries and narrative Diagnostic Imaging reports are delivered directly to the patient's chart for their clinician to access in a timely and less labour-intensive manner.

3. Accountability

The Chief Executive Officer (CEO) is responsible for managing privacy protection, including ensuring that OntarioMD complies with applicable privacy requirements. The CEO delegates responsibility to OntarioMD's Chief Privacy Officer to:

- Lead the design and operation of the OntarioMD privacy framework;
- Provide advice, support and direction to personnel about privacy matters applicable to their areas of responsibility; and
- Monitor and reports on privacy protection at OntarioMD.

OntarioMD shall provide its personnel and third-party providers with formal direction on their accountabilities, roles and responsibilities for protecting privacy. Means of providing such direction may include training and awareness programs, agreements, written policies and procedures, and job descriptions.

OntarioMD personnel and third parties are responsible for achieving and demonstrating compliance with privacy requirements applicable to their areas of responsibility.

4. Restricted and Controlled Access to PI and PHI

OntarioMD personnel and third parties shall not access personal information (PI) and personal health information (PHI) unless:

- Access is necessary in order to perform their roles;

- Authorization has been given by the requisite authority;
- Applicable privacy training has been completed and applicable agreements have been signed;
- Compliance with any additional privacy-related requirements and restrictions established by OntarioMD have been formally agreed to; and
- Compliance with all applicable policies has been confirmed.

In addition, a formal user registration and de-registration procedure are in place for granting and revoking access to all information systems and services. Separation of duties, roles, and access levels are in place for different groups to ensure that users have access to PI or PHI only on an as needed basis.

5. Obligations and Responsibilities of the Parties

Authorized users of HRM shall comply with the obligations imposed by PHIPA, applicable privacy policies and agreements.

6. Administrative Safeguards

Authorized end users participating in HRM are required to sign agreements that outline their obligations and responsibilities with respect to the collection, use and disclosure of PI and PHI.

OntarioMD personnel are required to sign confidentiality agreements and undergo annual training on privacy and security. All personnel are required to report incidents through OntarioMD's internal process for reporting and managing privacy incidents, which are reviewed by the Chief Privacy Officer and their delegates.

7. Technical Safeguards

- Hardware and software including the Operating Systems (OS) are built and hardened for security in accordance with Ontario Health policies, processes and standards
- HRM leverages Ontario Health's secure multi-zone infrastructure and is designed to be a multi-tier application where different components reside in different zones. Access is controlled at different levels and only via secure channels.
- All related transactions are logged at different levels (OS, applications, etc.), including administrative and client access.
- Data is transmitted from the sending facilities to HRM over either Ontario Health's ONE Network or ONE Access Gateway, both of which are designed to meet the privacy and security needs that the exchange of electronic patient information requires.HRM data exchange with receiving facilities is managed through controlled, authenticated, and encrypted access mechanisms that help ensure information is transmitted only between authorized facilities and systems.
- Files within HRM that are older than 28 days are purged from HRM with a notification sent to the related facilities.
- Retention of transacted PHI data is generally limited to 28 days, with automated purging mechanisms in place.

8. Physical Safeguards

Production HRM systems are hosted in Ontario Health-managed environments that are designed and operated to support the secure handling of PHI. Strict policies and procedures enforce physical safeguards in areas such as:

- Physical access to the hosting environments
- Secure remote access to the hosting environment
- Change and release management procedures
- Secure and redundant design of the computing environment and the HRM system.

9. Openness

OntarioMD's privacy policies and practices are published on the OntarioMD website which can be easily accessed at https://www.ontariomd.ca. The following policies are readily available on the OntarioMD website at https://www.ontariomd.ca/products-and-services/health-report-manager/documentation:

- OntarioMD Health Report Manager Privacy Policy:
- OntarioMD Privacy Breach Management Policy;
- OntarioMD Privacy Complaints and Inquiry Policy and Procedures; and,
- Summary of Health Report Manager Privacy Impact Assessment.

10. Incident Management and Reporting

All privacy incidents must be reported to the OntarioMD Chief Privacy Officer as stipulated in the OntarioMD Privacy Breach Management Policy. The OntarioMD Chief Privacy Officer is responsible for reviewing and managing all reported incidents. The Chief Privacy Officer will also notify the appropriate health information custodian (HIC) of a suspected privacy breach, as appropriate. Patient notification of the privacy breach will be handled by the applicable HIC by following its internal incident reporting processes.

Under Ontario Reg. 329/04, a HINP is required to notify every applicable HIC at the first reasonable opportunity if it detects any unauthorized access, use, disclosure or disposal of personal health information.

11. Challenging Compliance

An individual may register a complaint in writing by contacting:

OntarioMD Chief Privacy Officer
150 Bloor St. West, Suite 900
Toronto, ON M5S 3C1

All complaints will be reviewed and will receive a response.

An individual may also submit a concern or complaint in writing to the Information and Privacy Commissioner of Ontario by contacting:

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, ON
M4W 1A8