Privacy Policy

Hospital Report Manager

Version: 0.3

Table of Contents

Document Control

Review Frequency:	Biennially or at greater frequency at the discretion of the Privacy Officer

Approval History

Approver(s)	Approved Date
Sarah Hutchison, Privacy Officer, OntarioMD	August 29, 2013

Revision History

Version No.	Version Date	Summary of Change
0.1	July 20 2012	First Draft
0.2	June 3, 2013	Gosia Kacprzak - consistency review
0.3	June 17, 2013	Kathy Tudor – general editing and corporate communications

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 Hospital 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

The HRM is an OntarioMD managed application that enables hospitals to electronically transmit patient reports to their practice-based clinician's Electronic Medical Record (EMR) for inclusion in follow-up care. This solution replaces the existing 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 the introduction of HRM, hospital reports are updated directly to the patient's chart for their clinician to access in a timely and less labour intensive manner.

3. Accountability

3.1 Roles and Responsibilities

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 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 report 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 employees 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

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 only have access to PI or PHI on an as needed basis.

5. Obligations and Responsibilities of the Parties

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

6. Administrative Safeguards

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

OntarioMD requires the completion of confidentiality agreements and privacy training for all personnel and third parties that could potentially have access to PI and PHI.

7. Technical Safeguards

- Hardware and software including the Operating Systems are built and hardened for security in accordance with eHealth Ontario policies, processes and standards
- HRM leverages eHealth Ontario’s secure multi-zone infrastructure and is designed to be a multi-tier application where different components reside in different zones. A different set of enterprise firewalls separate the DMZ from the MPN and the Internet.
- 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 clients access.
- Data is transmitted from the sending facilities to the HRM over eHealth Ontario's private ONE Network, which is designed to meet the privacy and security needs that the exchange of electronic patient information requires. If the transmission channel is over the Internet, then IPsec VPN site-to-site tunnel will be established per sending facility.
- Firewalls will restrict access to each registered sending facility based on their IP addresses and special designated TCP port(s).
- Encrypted files are downloaded by the receiving facility over the public Internet using SSH2 protocol.
- Receiving facilities are restricted per their Electronic Medical Record instance, the source IP, and the special SSH key and their files encryption/decryption key.
- Files within the HRM that are older than 28 days are purged from HRM with a notification sent to the related facilities.

8. Physical Safeguards

HRM systems are hosted at the Ministry of Health's Guelph Data Centre (GDC) which has a disaster recovery site located at Streetsville Computing Center - Disaster Recovery (SDC). eHealth Ontario is managing the related Operating Systems and infrastructure components while OntarioMD is managing the HRM applications.

- HRM equipment resides in a specially-built facility that is physically and logically secured to prevent unauthorized access. HRM equipment is located in isolation from other health information systems.
- The hosting facilities have multiple layers of safeguards and are staffed and monitored 24/7 by security personnel.
- The facility protects against environmental issues such as power outages and extreme weather conditions.
- Physical access to the systems is restricted to authorized personnel only. Raise floor access is permitted via finger print and card reader access. OntarioMD personnel do not have any physical access but can remotely access the application using Citrix.

9. Training

OntarioMD personnel, authorized end users of HRM and third parties are provided with privacy education.

10. Openness

OntarioMD's privacy policies and practices are published on the OntarioMD website which can be easily accessed at www.ontariomd.ca/ir/hrm. Printed copies are also available through the Privacy Officer. The following policies are readily available on the OntarioMD website:

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

11. Incident Management and Reporting

All privacy incidents must be reported to the OntarioMD Privacy Officer as stipulated in the OntarioMD Privacy Breach Management Policy. The OntarioMD Privacy Officer is responsible for advising the OntarioMD CEO of any reported incidents. The Privacy Officer will also notify the appropriate HIC(s) 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.

12. Challenging Compliance

An individual may register a complaint in writing by contacting:

OntarioMD 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