Central Intake Program

Privacy Policy

Version: 0.1

Table of Contents

Program Overview

The Central Intake Program (CIP) is a program hosted by Halton Healthcare and funded by the Mississauga Halton LHIN. The program operates as a single access point and manages referrals to community diabetes education programs, diabetes foot care program, self-management program and addiction & mental health services in the Mississauga Halton LHIN region. Central Intake receives triages and directs referrals to the appropriate program based on patient demographics and service needs.

The eReferral solution is an online application that enables Healthcare providers to electronically submit and track their referrals. The application will also be utilized by the Central Intake Program to receive the referral and route to the appropriate service provider. The eReferral solution will replace the existing process of paper referrals and faxes being sent to the service provider's office.

The Central Intake Program understands the importance of ensuring the privacy of the personal health information it collects and shares with partnering healthcare providers as part of the circle of care. We are committed to respecting personal privacy, and managing the security of the personal health information within our eReferral application.

Collection, Use and Disclosure of Personal Health Information

Ontario Privacy Legislation, the Personal Health Information Protection Act, 2004 establishes rules concerning the collection, use and disclosure of personal health information by health information custodians and other persons.

Under the Personal Health Information Protection Act, 2004, MH CIP eReferral operates as a "Health Information Network Provider" & "Agent" to participating health information custodians who contribute data to the Central Intake eReferral 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)

The Central Intake Program completed a comprehensive privacy impact assessment in October 2014 to ensure that the eReferral solution met the requirements of PHIPA

The following safeguards have been implemented to protect personal health information.

Restricted and Controlled Access

Personnel and third parties shall not access personal information or personal health information unless:

- Access is necessary in order to perform their roles
- Authorization has been given by the requisite authority;
- Applicable agreements have been signed;
- Compliance with all applicable polices have been confirmed

Administrative Safeguards

- MHCIP has appointed designated individuals for privacy and security.
- MHCIP has a comprehensive set of information security policies, which are regularly revised and updated. Staff members and contractors are required to read the relevant policies and sign an attestation that they have read, understood and are committed to complying with them.
- All staff and contractors must sign confidentiality agreements and undergo background checks prior to joining or providing services to MHCIP.
- MHCIP conducts mandatory privacy and security awareness training programs for staff, which includes a quiz to confirm that the main concepts and behavior requirements were understood.
- All privacy and security incidents are managed in accordance with MHCIP Incident Management Policy.
- Threat and risk assessments are conducted whenever new projects are undertaken or change in security architecture is introduced.
- MHCIP provides a written copy of the results of privacy impact assessments and security threat and risk assessments to the affected health information custodians.
- MHCIP has established a formal threat and risk management program. A specialized management forum, the security leadership group, provides strategic direction and governance oversight for the risk-management program, including regular review of risks and the corresponding risk treatment plans.
- Audit logs recording user activities, system administrator's activities, exceptions, and information security events are kept and archived.

Technical Safeguards

- Strong authentication mechanisms are enforced for accessing sensitive systems.
- Administrative access to information-processing infrastructure is granted on a need to know basis. All system and application access activities are logged.
- Network traffic is monitored and managed using security devices such as routers, switches, network firewalls, intrusion-detection systems and anti-virus programs.
- End-to-end encrypted channels are used for all data communication between MHCIP and its member sites.
- Vulnerability assessments of technical configurations and operational security practices are carried out periodically and when new projects are undertaken or significant changes are introduced.
- A patch management process ensures that the information-processing infrastructure is updated with critical security patches and functional updates in a timely manner.
- All accounts of former staff or consultants are revoked upon termination of employment or contracts.
- Critical information is backed up on a regular basis and is recoverable in case of operational incidents.
- Infrastructure availability is monitored and managed 24/7.

Physical Safeguards

- MHCIP eReferral infrastructure is hosted in secure data centre facility that is well equipped with applicable environmental controls.
- Physical access to the data-centre is restricted to authorized users only, and facility is manned and supervised 24/7.
- Only authorized staff members and contractors are permitted access to MHCIP office areas.
- All Visitors to MHCIP office are escorted at all times by staff members.
- All equipment that was used to store or process PHI is securely disposed in accordance with Halton Healthcare Destruction of PHI Policy.
- Policy, procedures and required equipment resources are in place for secure disposal of sensitive information stored on paper, CDs, or other such media.

Challenging Compliance

A patient will be able to address a challenge concerning compliance with the above principles to the Privacy Officer, who is accountable for Halton Healthcare compliance.

Openness

Central Intake will be open and make readily available to individuals, specific information concerning the programs policies and practices with respect to the management of personal information. These will be available in a form that is generally understandable and easily accessible. The information made available will include:

- Name, title and address of the Privacy officer
- eReferral Threat Risk Assessment
- Referral Privacy Impact Assessment
- Breach Management Policy
- Privacy Policy

Obligations and Responsibilities of the Parties

Authorized users of the eReferral system shall comply with the obligations imposed by PHIPA, as well as all applicable privacy policies and agreements.

Incident Management and Reporting

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.

All privacy incidents must be reported to the Halton Healthcare Privacy Officer as stipulated in the Central Intake Privacy Breach Management Policy. The Privacy Officer is responsible for; advising the Central Intake manager of any reported incidents, as well as notifying the appropriate Health Information Custodian(s) of a suspected privacy breach. Patient notification of the privacy breach will be handled by the applicable Health Information Custodian by following internal incident reporting process.

Halton Healthcare will investigate all complaints. If a complaint is found to be justified, appropriate measures will be taken to rectify the situation, and shall be dealt with through the Halton Healthcare Progressive Discipline policy.

If a patient is not satisfied with the response from the Privacy Officer, he or she may have recourse to the Office of the Information and Privacy Commissioner of Ontario:

Phone 416-326–3333
commissioner@ipc.on.ca