Health Information Network Provider (HINP)

Ontario's *Personal Health Information Protection Act* (PHIPA) sets out rules for the collection, use and disclosure of personal health information (PHI) by health information custodians and it defines how health care providers, organizations and electronic hosting systems may collect, use and share personal health information (PHI).

In today's world, electronic information systems play an important role in provision of health care services. It is important that health care providers have timely access to information necessary for provision of care. When information is securely shared between healthcare providers this helps them provide best possible care.

CAMH is a Health Information Network Provider (HINP) when we provide services to two or more Health Information Custodians (HICs) where the services are provided primarily to custodians to enable the custodians to use electronic means to share personal health information with one another. When doing so, CAMH must comply with the HINP requirements set out in PHIPA and applicable regulations.

In its role as a HINP, CAMH hosts several electronic information systems that allow authorized health care providers to contribute to, store, access and share their patients' PHI. As we do so, we are committed to protecting your PHI.

As a HINP, CAMH hosts the following system:

DATIS

The Drug and Alcohol Treatment Information System (DATIS) has been an important tool used to monitor the availability and type of substance use services within Ontario. DATIS is a client-based information system that monitors the number and types of publicly-funded addiction treatment services in Ontario. It contains data from over one million people. DATIS allows service providers to provide the Ministry of Health and Long-Term Care and Local Health Integration Networks with data for policy, planning and accountability.

Directives, Guidelines and Policies

In hosting the above system CAMH will:

- enter into a written agreement with each HIC concerning the services provided
- use PHI of a HIC only to support the purposes and provide the specific services identified in its agreement with the HIC;
- not use PHI of a HIC for its own purposes;
- will limit access to and use of PHI by it's personnel to ensure that they only use or access PHI required to provide services to HICs;
- not disclose PHI of a HIC to any individual or third party unless authorized to do so by the HIC that is the custodian of the PHI or when permitted or required to do so by law;
- not alter PHI it manages on behalf of HICs in any way unless the alteration:
    - is described in CAMH's agreement with the HIC as an authorized use of the PHI, or
    - has been requested in writing by the HIC;

- conduct scheduled privacy audit activities to determine whether or not CAMH staff are in compliance with CAMH's privacy obligations as a Service Provider;
- provide HICs with the results of its privacy audits on request;
- conduct privacy audit activities at the request of a HIC, to support a HIC in managing or investigating a privacy incident or privacy complaint;
- support HICs in responding to privacy complaints that are received by HICs that relate to the services provided to the HICs by CAMH;
- notify participating HICs of any privacy breaches detected;
- maintain appropriate logging and monitoring of PHI that will be made available to participating HICs on request; and
- notify participating HICs of any privacy breaches detected.

In addition to the commitments above, the following internal policies, procedures and standards are also relevant to our governance of the above systems:

- Management of Personal Health Information and Personal Information
- Privacy Incident Management Protocol
- Retention and Storage of Records
- Storage of Personal Health Information/Personal Information on Mobile Computing Devices
- Information Security
- Access Control Standard
- Encryption Standard.
- Perimeter Security Standard
- Servers and Desktops Security Standard
- Physical and Environmental Security Standard

Organizational safeguards

CAMH has technical, physical and administrative safeguards in place to help protect against unauthorized use and disclosure on personal health information and to protect the integrity of the information in the above systems. These include but are not limited to:

- use of strong passwords that meet the organization's password complexity requirements
- multi-factor authentication (MFA) for all systems and applications whenever possible
- role-based access control system to manage user privileges effectively
- firewalls and intrusion prevention systems
- regular vulnerability assessments and penetration testing
- sensitive data classified according to its level of sensitivity and handled in accordance with applicable laws and regulations
- data encryption implemented for sensitive data in transit and at rest
- regular data backups performed and tested
- employee training on privacy awareness and security best practices
- Privacy Impact Assessments and Threat Risk Assessments

For more information and questions about our privacy and security practices, contact CAMH Information and Privacy Office at (416) 535-8501 ext. 33314 or by email at **privacy@camh.ca**