Canadian Mental Health Association Sudbury/Manitoulin *Mental health for all* / Association canadienne pour la santé mentale Sudbury/Manitoulin *La santé mentale pour tous*		**EMPLOYEE POLICIES** Category: **General Personnel**
Implementation: July 2018 **Reviewed / Revised / Approved**: July 2018	Number: AA-AG-P0047	**PRIVACY**

POLICY

In the course of delivering its services and programs, CMHA collects, uses and discloses personal health information from its individuals. CMHA is committed to protecting the confidentiality of individuals' personal health information and the privacy of the individuals while facilitating the effective provision of CMHA services and programs.

CMHA maintains privacy in compliance with the Personal Health Information Protection Act (PHIPA) 2004, which establishes rules for the collection, use and disclosure of personal health information about the individuals. All CMHA staff are responsible for the privacy and confidentiality of the personal health information that are collected, used and disclosed by CMHA.

CMHA established this privacy policy to specify the privacy requirements that apply to all CMHA staff and volunteers.

PROCEDURE

PRIVACY GOVERNANCE

The CEO has overall accountability for protecting the individual's privacy and ensuring compliance with the Personal Health Information Protection Act (PHIPA) 2004 and Regulation 329/04. The Director of Operations is accountable for ensuring that CMHA has established an effective and efficient privacy program. Specifically, the Director of Operations will, in conjunction with the Privacy Officer:

- Oversee the execution of the privacy program to support the compliance of the staff with CMHA's privacy policies and practices.
- Oversee the execution of the privacy program to support the compliance of CMHA's employees, contractors, affiliated physicians and their employees with the privacy policies and practices.
- Review performance of the privacy program, and
- Provide guidance on the resolution of privacy issues, including but not limited to:
    - privacy complaints
    - privacy breaches
    - results of privacy reviews, audit and assessments
    - recommendations for changes to CMHA's privacy policy and practices

Privacy Officer

The Privacy Officer is responsible for:

- Maintaining knowledge of privacy legislation and regulations

- Ensuring that CMHA complies with its privacy obligations as defined in PHIPA 2004, Regulation 329/04, other relevant legislation, and its own policies
- Establishing and managing CMHA's privacy processes and education
- Preparing the annual plan for CMHA's privacy and reporting on privacy and security
- Communicating the privacy policy to the general public
- Developing and publishing privacy notices, as required
- Delegating responsibility for ensuing that third party service providers are compliant with the privacy terms of their agreements
- Monitoring compliance with CMHA's privacy policy and privacy legislation and regulation
- Conducting audit and/or assessment of the privacy management and operations to identify non-compliance issues, gaps and deficiencies as well as opportunities for improvement.
- Overseeing regular audits of staff's collection, use and disclosure of personal health information to detect suspicious activities.
- Managing privacy related issues according to established procedures
- Responding to requests for access and correction, ensuring that employees are aware of privacy concepts and principles, relevant legislation and CMHA's privacy policies and practices
- Providing privacy guidance to all CMHA projects and staff on an as-needed basis
- Liaising with other organizations, the public and government, as necessary, on privacy-related issues.
- Acting as the point of contact for, and managing privacy inquiries and complaints made under Personal Health Information Protection Act and its regulation
- Managing, the containment, resolution and investigation of privacy breaches

In conjunction with the Director of Operations:

- Directing privacy reviews, assessments and audits
- Maintaining a risk registry to monitor privacy related issues and risk mitigation activities
- Maintain an action plan to continuously improve CMHA privacy management policies and practices

PRIVACY POLICY

1. Legal Obligations

1.1 As a health information custodian (HIC), CMHA and their agents (including employees, physicians, contractors, consultants, volunteers, students and other workers at CMHA, and all personnel affiliated with third-parties who provide services to CMHA) are responsible for ensuring that the personal health information (PHI) of the individuals is treated according to the requirements set out in Personal Health Information Protection Act 2004 and its regulation.

2. Consent for the Collection, Use and Disclosure of Personal Health Information

2.1 The knowledgeable consent of the individual or substitute decision maker (SDM) is required for the collection, use or disclosure of personal health information, except as set out in this policy or permitted or required by law.

2.2 The individual or SDM should be informed of:

a) the personal health information collected, used and disclosed by CMHA; the purposes for collection, use and disclosure;

b) how the personal health information is being collected, used and disclosed and with who;
c) the individual's right to give or withhold consent, access or correct the personal health information, and inquire or complain about CMHA's privacy practices; and
d) the positive or negative consequences of giving, withholding or withdrawing consent.

2.3 The implied consent of individuals is sufficient for the disclosure of personal information to other health information custodians for the purposes of providing health care.

2.4 The expressed consent of individuals should be obtained
a) for disclosures to people or organizations that are not health information custodians as defined by the Personal Health Information Protection Act 2004;
b) for disclosures to health information custodians that are not for the purpose of providing health care; and
c) for uses and disclosures the purpose for which was not communicated when consent was initially obtained by CMHA.

2.5 Individuals are able to withhold or withdraw their consent to the collection, use and disclosure of their personal health information at any time. The CMHA staff will respect an individual's right to request that her or his personal health information be withheld from specific individuals and organizations, and will take reasonable measures to ensure that personal health information is withheld from the specified individuals and organizations.

2.6 CMHA will not disclose the personal information of individuals without their consent, except where:
a) It is believed that there is an imminent risk of significant harm, (refer to Duty to Warn and Involuntary Assessment policy and Rapid Mobilization Table referral documents for examples)
b) A child aged 16 or under is at risk or has been abused or neglected (see Child Abuse policy).
c) The agency is subpoenaed or is otherwise served with a court order, summons, warrant or a similar requirement issued by a person who has jurisdiction to compel the production of information in a proceeding, or it is otherwise permitted or required by law. This includes:
    - a proceeding held in, before or under the rules of a court,
    - a tribunal, a commission, or an arbitrator,
    - a justice of the peace or a coroner,
    - a committee of a College within the meaning of the *Regulated Health Professions Act, 1991*, and
    - Health conditions of the individual may make it dangerous to operate a vehicle or perform duties, as required under the *Highway Traffic Act* and the *Aeronautics Act*.

2.7 If CMHA staff are served with a warrant, summons, subpoena, order or similar requirement issued in a proceeding, the individual must:
- Immediately notify their manager, who will provide advice and direction as to how to respond following consultation with the Privacy Officer. In general, where an order, summons, warrant, subpoena or other requirement to produce documents has been served on CMHA, CMHA will comply with the order in the appropriate timeframe,

2.7 Where CMHA discloses personal information without the individual's consent, the individual will be notified of such disclosure as soon as reasonable, practical, safe and/or legally possible in the circumstances. CMHA will make an exact copy of the file to remain at the agency, and securely deliver the documents to the court or other proceeding.

3 Limiting the Collection, Use and Disclosure of Personal Health Information

3.1 At or before the time personal health information is collected, CMHA will identify the purposes for which the personal health information is collected.

3.2 Permitted purposes for which the personal health information is collected, used and disclosed include:

a) Providing quality healthcare programs and services to individuals;
b) Providing information to other people or organizations who are within the Circle of Care that is necessary and required for the facilitation of healthcare services;
c) Conducting research to understand the needs of individuals and contribute to continuous quality improvement;
d) Reviewing individual files to ensure high quality of service and documentation;
e) Evaluating the effectiveness of agency programs and services; and
f) Meeting legal and regulatory requirements.

3.3 CMHA will limit the collection, use and disclosure of personal health information to only the information that is required to fulfill the purposes that were identified to individuals before collection.

4 Retention, Archiving and Destruction of Personal Health Information

4.1 All personal health information should be retained only for the time period required to fulfill the purposes for which the information was collected, or as authorized or required by legislation.

4.2 Personal health information should be retained for 15 years or 10 years after the individual becomes 18.

4.3 Personal health information that is no longer required by CMHA for its identified purposes should be securely destroyed or rendered irretrievable to prevent unauthorized access to the information

5 Openness

5.1 CMHA will make available to the public the information regarding its privacy practices.

5.2 CMHA will publish the contact information for privacy matters on CMHA's public website and other individual communication materials.

6 Individual's Privacy Rights

6.1 CMHA will inform the individual of the existence, use and disclosure of his or her personal health information upon request, and will give the individual access to that information pursuant to Access and Correction procedures.

6.2 The right of individual's access does not apply when:

a) A record was created for quality assurance purposes, or contains quality of care information or raw data from a standardized psychological test or assessment;
b) A record is subject to a legal privilege or other legal restriction;
c) Granting access could be reasonably expected to create a risk of harm to the individual or another person;
d) Granting access could be reasonably expected to lead to the identification of a person who was legally required to provide information for the record, or a person who provided information in confidence;
e) Personal health information used solely for research purposes; or
f) Personal health information that is in the custody or control of a laboratory for a test requested by a health care practitioner, where an individual has the right to access that information from

the health care practitioner and the practitioner has not directed the lab to provide the information directly to the individual.

6.3 CMHA may charge a fee not exceeding reasonable cost recovery for providing access to an individual's record of personal health information.

6.4 CMHA will correct the individual's personal health information or record a Statement of Disagreement upon request.

6.5 CMHA will accept inquiries and complaints regarding its privacy practices from any individual or organization. The Privacy Officer will review and respond to all privacy inquiries and complaints.

7 Ensuring Accuracy of Personal Health Information

7.1 CMHA will take reasonable steps to ensure that personal health information under its control is accurate, complete and relevant as is necessary to minimize the possibility that inappropriate information may be used for a specified purpose.

7.2 An individual will be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

8 Safeguards

8.1 CMHA will implement appropriate information security safeguards to protect personal health information from unauthorized collection, use or disclosure, including:

a) administrative safeguards such as privacy and security training and awareness activities
b) technical safeguards such as encryption of personal health information
c) physical safeguards such as locked cabinets for paper records

9 Breach Management

9.1 CMHA staff will receive training in supporting the containment, resolution and investigation of privacy breaches within the CMHA.

9.2 CMHA will execute a breach management procedure to manage the privacy breach appropriately, which includes:

a) containing the incident;
b) investigating the incident to determine the nature, scope and root cause of the incident;
c) evaluating the cause(s) of the incident and conducting remediation activities as required.

9.3 CMHA must notify the individual at the first reasonable opportunity following theft, loss or unauthorized use or disclosure of their PHI.

9.4 CMHA must notify the Information and Privacy Commissioner of Ontario (IPC) of theft, loss or unauthorized use or disclosure of Personal Health Information.

9.5 In the event of a privacy breach committed by a CMHA employee who is also a member of a professional regulatory college, CMHA must notify the professional regulatory college of any termination, suspension, or disciplinary action taken against the employee as a direct result of that breach.. College reporting is also required where CMHA has reasonable grounds to believe that an employee's resignation is related to an investigation or other action related to a privacy breach.

9.6 CMHA must track privacy breach statistics, and must report them annually to the Information and Privacy Commissioner of Ontario (IPC) .

10 Training and Awareness

10.1 As a condition of employment, all CMHA staff must sign a confidentiality and privacy agreement.

10.2 All third party vendors and affiliated personnel who provide services to CMHA must sign a confidentiality agreement.
10.3 CMHA will make its employees aware of privacy concepts and principles, provincial legislation and CMHA privacy policies and practices.
10.4 CMHA will provide ongoing training and awareness to ensure staff and personnel affiliated with third party vendors or service providers are provided with the tools, training and support as appropriate to enable them to fulfill their duties as it relates to the individual's privacy.

Discipline Action
Any breach of Privacy Policies will result in disciplinary action up to and including termination.

POLICY MAINTENANCE
While this Policy is expected to be long-term, changes will be needed to keep it up to date with changes in both internal and external environments. This Privacy Policy will be reviewed on a periodic (at least annually) basis and revised as needed.

REFERENCE DOCUMENTS

- Privacy & Confidentiality Agreement & Pledge

DEFINITIONS

Terms	Definition
CMHA Staff	CMHA staff including fulltime employees, contracted personnel, the affiliated physicians, students and volunteers.
Collect	As defined in section 2 of Personal Health Information Protection Act 2004, "collect" means to gather, acquire, receive or obtain the information by any means from any source, and "collection" has a corresponding meaning.
Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
Consent	Consent is defined in Personal Health Information Protection Act 2004 PART III, under sections 18 – 28. Under Personal Health Information Protection Act 2004 section 18(1)(b) in order for consent to be valid; consent must be knowledgeable. Knowledgeable consent is defined in section 18(5) as: A consent to the collection, use or disclosure of personal health information about an individual is knowledgeable if it is reasonable in the circumstances to believe that the individual knows, • the purposes of the collection, use or disclosure, as the case may be; and that the individual may give or withhold consent. 2004, c. 3, Sched. A, s. 18 (5). Consent can be either implied or express, but in order to be valid the consent must be knowledgeable.

Consent Directive	An individual's request to place restrictions on the use or disclosure of his/her personal health information by either expressly withdrawing or withholding consent is referred to as a "consent directive." Consent directives are implemented through "blocking" mechanisms in the EMR or physical restriction to access the personal health information record on non-electronic format such as paper records.
Disclose	As defined in section 2 of Personal Health Information Protection Act 2004, "disclose" refers to making personal health information "available" or "to release it to another health information custodian or to another person."
Express consent	"Express consent" means asking a individual to expressly provide his/her permission (which may be provided either orally or in writing) to collect, use or disclose his/her personal health information.
Health Information Custodian ("HIC")	"Health information custodian", subject to subsections (3) to (11) of Personal Health Information Protection Act 2004, means a person or organization described in personal health information PA who has custody or control of personal health information as a result of performing the person's or organization's powers or duties. (See personal health information PA for a complete definition.)
Implied consent	Implied consent refers to situations in which it is reasonable to infer that the individual is consenting by the action that they have taken, and it is not necessary to specifically (or expressly) ask for the individual's consent. For example, when a individual allows their blood to be drawn at a medical laboratory, it is implied that they consent to the results of their blood work to be disclosed to the ordering clinician. Similarly in community care, when a individual fills out an intake form that clearly identifies the purposes of the form and what it will be used and who it will be shared with.
Personal Health Information (PHI):	Identifying information about an individual in oral or recorded form, if the information as referenced in Personal Health Information Protection Act, 2004: • Relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family; • Relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual; • Is a plan of service within the meaning of the Home Care and Community Services Act 1994, for the individual; • Relates to the donation by the individual of any body part of bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance; • Is the individual's heath number; or, • Identifies an individual's substitute decision maker.
Personal Information (PI):	Personal information includes personal health information and any factual or subjective information, recorded or not, about an identifiable individual. This includes information in any form, such as: • age, name, ID numbers, income, ethnic origin, or blood type; • opinions, evaluations, comments, social status, or disciplinary actions; and • employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, intentions (for example, to acquire goods or

	services, or change jobs) Personal information does not include the name, title or business address or telephone number of an employee of an organization.
Personal Health Information Protection Act (PHIPA) 2004	The Personal Health Information Protection Act, 2004, S.O. 2004, c.3, Schedule A is Ontario legislation governing OTN's collection, use and/or disclosure of personal information / personal health information.
Regulation	Ontario Regulation 329/04 made under Personal Health Information Protection Act 2004.
Privacy	The right of an individual to control the collection, use and disclosure of his/her Personal Information; freedom from intrusion into the private life or affairs of an individual when that intrusion results from undue or illegal gathering and use of data about that individual.
Privacy Breach	A privacy breach may take the following forms: • The collection, use, and disclosure of personal health information that is not in compliance with the Act or its regulation; • A contravention of the privacy policies, procedures or practices implemented by a prescribed person; • A contravention of agreements involving Personal Information /Personal Health Information including Third Party Service Providers retained by CMHA Peel; and Circumstances where personal health information is stolen, lost or subject to unauthorized use of disclosure or where records of personal health information are subject to unauthorized copying modification, or disposal.
Privacy Impact Assessment (PIA)	A PIA is a formal risk management tool used to identify the actual or potential effects that a proposed or existing information system, technology or program may have on individuals' privacy. A PIA also identifies ways in which privacy risks can be mitigated.
Substitute Decision Maker (SDM)	A substitute decision maker is an individual authorized under section 5 of Personal Health Information Protection Act 2004to consent on behalf of a individual to the collection, use or disclosure of personal health information about that individual. As such, all references to an "individual" made in this document are also inclusive of authorized SDM's.
Threat Risk Assessment (TRA)	A Threat and Risk Assessment is a formal tool to provide senior management of an organization with the necessary information to make decisions on risks, based on a review of the information holdings and systems under assessment.
Use	As Defined in section 2 of Personal Health Information Protection Act 2004, "use" means "to handle or deal with personal health information." The definition of use is distinct from, and should not be confused with, the term "disclose" (see above).

AUTHORITY: CEO