Canadian Mental Health Association Manitoba and Winnipeg *Mental health for all*	Approval Signature: 	Page **1** of **7** **Addenda** Pledge of Confidentiality Personal Health Information Access Personal Health Information Withdrawal
Section 1 **Policy No. 1.3**	Date: **October 15, 2021**	Supersedes: **January 27, 2020** **July 8, 2013**
Confidentiality of Personal Health Information		

PURPOSE

To ensure that the Canadian Mental Health Association Manitoba and Winnipeg (CMHA) protects Personal Health Information including demographic Information so that Individuals are not afraid to seek health care or to disclose sensitive information to health professionals.

To also ensure that Personal Health Information is protected during its collection, use, disclosure, storage, and destruction in accordance with the provisions of *The Personal Health Information Act (PHIA)* and other prevailing enactments such as *The Mental Health Act*.

DEFINITIONS

"Personal information" means information about an identifiable individual (e.g., name, age, date of birth, home address, e-mail address, phone number, social insurance number, marital status, ethnicity, income, medical and health information, education, employment information, banking information, credit card information, and emergency contact information). Personal information does not include business contact information (described below).

"Business contact information" means information that would enable an individual to be contacted at a place of business and includes name, position name or title, business telephone number, business address, business email or business fax number. Contact information is not covered by this policy or PHIA.

"Individual" includes participants (any individual receiving services or products from CMHA), participants, customers, members, volunteers, employees, and donors.

POLICY

All employees and persons associated with CMHA are responsible for protecting all Personal Health Information (oral or recorded in any form) that is obtained, handled, learned, heard, or viewed in the course of their work or association with CMHA. Communication of, or access to such information, is acceptable only in the discharge of one's duties and responsibilities (including duties imposed by legislation) and **based on the need to know**.

Discussion regarding Personal Health Information shall not take place in the presence of persons not entitled to such information or in public places (elevators, lobbies, cafeterias, off premises, etc.).

As a condition of employment/contract/association/appointment, all employees and persons associated with CMHA shall complete a Pledge of Confidentiality. The CMHA Pledge of Confidentiality shall be signed each time there is a substantial change in an individual's position, as determined by the program manager/director responsible for the position.

Personal health Information shall be protected during its collection, use, storage, and destruction within the Agency.

All contractors engaged in providing a service for the Agency, where the service provided would expose them to confidential information, shall be required to sign a contract that provides, amongst other things, for the protection of confidential information including Personal Health Information.

All employees and those persons regularly associated with CMHA with access to personal information about participants and/or employees of CMHA will respect individuals' rights to total privacy concerning the details of their lives such as their addresses, backgrounds, family relationships and all personal health information.

1. Collecting Personal Information

Unless the purposes for collecting personal information are obvious and the individual voluntarily provides their personal information for those purposes, we will communicate the purposes for which personal information is being collected, either orally or in writing, before or at the time of collection.

We will only collect personal information that is necessary to fulfill the following purposes:

- To verify identity
- To identify participant preferences
- To understand the needs of our participants
- To enroll the participant in a program or service
- To ensure a high standard of service to our participants
- To issue tax receipts
- To contact and thank volunteers and supporters
- To organize employee payroll
- To screen volunteers
- To schedule volunteer activities
- To deliver services
- To award education bursaries
- To elect Board Members
- To keep members informed and up to date on our activities, special events and opportunities
- To register individuals for workshops and conferences
- To meet regulatory requirements

2. Consent

We will obtain individual consent to collect, use or disclose personal information (except where, as noted below, we are authorized to do so without consent).

Where possible we will collect personal information directly from the individual. In cases where consent for collection is required, we may collect an individual's personal information from another source with the individual's consent.

Consent can be provided orally, in writing, electronically, through an authorized representative or it can be implied where the purpose for collecting using or disclosing the personal information would be considered obvious and the individual voluntarily provides personal information for that purpose.

Consent may also be implied where an individual is given notice and a reasonable opportunity to opt-out of their personal information being used for mail-outs or the marketing of new services or products and the individual does not opt-out.

Subject to certain exceptions (e.g., the personal information is necessary to provide the service or product, or the withdrawal of consent would frustrate the performance of a legal obligation), individuals can withhold or withdraw their consent for CMHA Manitoba and Winnipeg to use their personal information in certain ways. An individual's decision to withhold or withdraw their consent to certain uses of personal information may restrict our ability to provide a particular service or product. If so, we will explain the situation to assist the individual in making the decision.

We may collect, use, or disclose personal information without the individual's knowledge or consent as outlined in sections 12, 15, and 18 of PIPA, including but not limited to the following circumstances:

- When the collection, use or disclosure of personal information is permitted or required by law.
- In an emergency that threatens an individual's life, health, or personal security.
- When a reasonable person would consider that it is clearly in the interests of the individual and consent cannot be obtained in a timely way.
- When the personal information is available from a public source.
- When the information is used to decide whether an individual is suitable for an honour, award or other similar benefit including scholarships or bursaries.
- When we require legal advice from a lawyer.
- For the purposes of collecting or paying a debt.
- To protect ourselves from fraud.
- To investigate an anticipated breach of an agreement or a contravention of law.
- When another Act or regulation requires or allows for the collection of information without consent (e.g., collecting an employee's social insurance number as required by the Income Tax Act to issue a T-4 slip).
- Where the information is necessary to collect or pay a debt owed to or by CMHA.
- Where consent is not required for disclosure (e.g., the disclosure is for the purpose of complying with a subpoena, warrant or order issued or made by a court; the disclosure is to law enforcement to assist in an investigation).
- To contact next of kin or a friend of an injured, ill or deceased individual.
- For employment purposes.
- For research or statistical purposes in certain circumstances.
- When we collect/use/disclose information from on or behalf of another organization (to which the individual previously gave consent), as long it's for the purpose for which it was originally collected and is to assist us in carrying out our work on behalf of that organization.

3. Using and Disclosing Personal Information

We will only use personal information where necessary to fulfill the purposes identified at the time of collection or for a purpose reasonably related to those purposes such as:

- To conduct surveys in order to enhance the provision of our services; and
- To contact our participants directly about products and services that may be of interest.
- We will not use or disclose personal information for any additional purpose unless we obtain consent to do so.
- We will not sell, rent, or trade participant lists or personal information to other parties.
- When CMHA provides information to research bodies performing studies on mental health populations, the data is in aggregate form and not personally identifying, so individuals remain anonymous. Any disclosure of information is compliant with Section 21 of PIPA.

4. Retaining Personal Information

If we use individual personal information to make a decision that directly affects the individual, we will retain that personal information for at least seven years so that the individual has a reasonable opportunity to request access to it.

Subject to the seven-year retention requirement, we will retain personal information only as long as necessary to fulfill the identified purposes or a legal or business purpose.

5. Ensuring Accuracy of Personal Information

We will make reasonable efforts to ensure that personal information is accurate and complete where it may be used to make a decision about the individual or disclosed to another organization.

Individuals may request correction to their personal information in order to ensure its accuracy and completeness. A request to correct personal information must be made in writing and provide sufficient detail to identify the personal information and the correction being sought.

If the personal information is demonstrated to be inaccurate or incomplete, we will correct the information as required and send the corrected information to any organization to which we disclosed the personal information in the previous year. If the correction is not made, we will note the individual's correction request in the file.

6. Securing Personal Information

We are committed to ensuring the security of personal information in order to protect it from unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks.

The following security measures will be followed to ensure that personal information is appropriately protected.

6.1 Physical Safeguards

- Personal information will be stored in locked filing cabinets.
- Employee access to storage areas or filing cabinets will be restricted to only those staff needing information as part of their official duties at CMHA.
- Files and documents containing personal information will not be left on desks when unattended (e.g., overnight).
- Cabinets where personal information is held will be physically secured (e.g., locking drawers).
- Files containing personal information will not be removed from the CMHA offices (e.g., employees will not take files containing personal information home to work on without the express permission of their direct manager and for a specific use).
- Where files containing personal information need to be transported (e.g., for an office move), a secure courier service should be used.

6.2 Administrative Safeguards

- We will provide training so that all employees know about and understand this privacy policy and PIPA's requirements for protecting personal information.
- All employees will read and sign CMHA 's Confidentiality Agreement regarding personal information.
- Personal information, especially sensitive information, will only be accessible to those employees who need to know the information.
- We will use role-based access to systems so that employees are only able to access personal information they need to perform their duties.
- Employees will use cover sheets when faxing personal information and will establish and follow procedures for ensuring only the authorized recipient has received the fax.

6.3 Technical Safeguards

- Employees will use password-protected computer screensavers so unauthorized personnel or visitors cannot see personal information.
- We will protect our computers and network by using firewalls, intrusion detection software, antivirus software, and by encrypting personal information.
- Employees will use strong and secure passwords to make sure that only authorized employees have access to computer storage devices or to the network. Employees will be prompted to change these passwords on a regular basis.
- Personal information stored on mobile electronic devices such as laptops or a USB flash drive will

be encrypted.

- All mobile devices (e.g., laptops and mobile phones) containing personal information must lock automatically and must require a password to unlock.
- Employees should not send personal information via e-mail. If personal information is received via e-mail, the receiver (employee) may respond but should de-identify the personal information, where possible (e.g., use participant initials instead of their full name) and should not provide additional personal information. The receiver may also advise the sender (participant or other employee) that email is not a secure method of communication.
- We will securely wipe all personal information from hard drives before they are discarded, sold, or donated.
- Secure databases which contain personal information require password login and have timeout forced logout when idle.
- We will use appropriate security measures when destroying individuals' personal information such as shredding documents and deleting electronically stored information.
- We will continually review and update our security policies and controls as technology changes to ensure ongoing personal information security.

7. Providing Individuals Access to Personal Information

Individuals have a right to access their personal information, subject to limited exceptions under section 23 of PIPA, which include but are not limited to:

- solicitor-participant privilege.
- where the disclosure would reveal personal information about another individual.
- where there are health and safety concerns.
- where the disclosure would reveal confidential commercial information; or where the disclosure would reveal the identity of an individual who provided information about another individual.

A request to access personal information must be made in writing and provide sufficient detail to identify the personal information being sought. A request to access personal information will be forwarded to the Privacy Officer for response.

Upon request, we will also tell individuals how we use their personal information and to whom it has been disclosed if applicable.

We will make the requested information available within Thirty (30) Business Days or provide written notice of an extension where additional time is required to fulfill the request.

A minimal fee may be charged for providing access to personal information. Where a fee may apply, we will inform the individual of the cost and request further direction from the individual on whether we should proceed with the request.

A fee will not be charged for an employee requesting their personal information.

If a request is refused in full or in part, we will notify the individual in writing, providing the reasons for refusal and the recourse available to the individual.

8. Contractors and Service Providers

As outlined in Section 1.2 Scope, this policy applies to all contractors and service providers collecting, using or disclosing personal information on behalf of CMHA.

In the event that we contract a third party to perform work for our organization, legally binding confidentiality agreements exist that commit those organizations to strictly adhere to CMHA's Privacy Policy and PIPA. Contracts with service providers will include the Privacy Protection Schedule.

9. Roles and Responsibilities

The protection of personal information is a responsibility shared by all.

All employees, including staff, management, and volunteers, are responsible for

- Complying with this policy and PIPA.
- Participating in privacy training provided by CMHA.
- Requesting clarification where needed.
- Reporting concerns, complaints and requests for information to the Privacy Officer.

Program Managers are responsible for

- Ensuring compliance with this policy and PIPA in their program.
- Responding to requests for information from participants in their program area and consulting with the Privacy Officer for guidance in responding.

The Privacy Officer is responsible for

- Ensuring CMHA 's compliance with this policy and the Personal Information Protection Act.
- Advising employees on specific questions relating to release of information and privacy.
- Reviewing and updating this policy regularly, or as PIPA is amended from time to time.
- Providing training and education to all employees.
- Supporting Branches in the implementation of privacy policies.
- Responding to complaints; and
- Liaising with the Office of the Manitoba Ombudsman where appropriate.

Program Managers, Directors, and the CEO are responsible for:

- Providing the time and resources for employees to attend training.
- Supporting employees in implementing this policy in their program or area.

Complaints and Requests for Information

CMHA is committed to having an accessible and responsive complaint-handling process in place to ensure individuals can make complaints about our organization's compliance with the Personal Information Privacy Act (PIPA).

Individuals should direct any complaints, concerns or questions regarding CMHA Manitoba and Winnipeg's compliance in writing to the Privacy Officer.

Stephanie Skakun, Privacy Officer
CMHA Manitoba and Winnipeg
930 Portage Avenue
Winnipeg, Manitoba R3G 0P8
T: 204-982-6110
E: sskakun@cmhawpg.mb.ca

If a complaint or request for information is made to CMHA, the following actions take place:

1. The date of the complaint or request for information is recorded and the receipt is immediately acknowledged in writing. The Privacy Officer is notified by the employee who received the complaint or request.

2. If necessary, the individual is contacted to clarify the nature of the complaint or request.

3. If it is a complaint, the Privacy Officer investigates, fairly and impartially. The individual is notified of the outcome of the investigation clearly and promptly and informed of any relevant steps taken to address their complaint. The complainant will receive a response within Thirty (30) Business Days.

4. If it is a request for information, the Program Manager may respond in consultation with the Privacy Officer. The requester will receive a response within Thirty (30) Business Days.

5. Where applicable, inaccurate personal information is corrected, and policies and procedures may be

modified based on the outcome of the complaint.

6. The date of response and outcome are recorded by the Privacy Officer.

7. All complaints received by the Privacy Officer will be included in an annual report made by the Chief Executive Officer.