Canadian Mental Health Association
North and West Vancouver
Mental health for all

Privacy Policy

Scope
This privacy policy applies to the Canadian Mental Health Association, North and West Vancouver (CMHA-NWV), including all employees, volunteers, programs and services. This policy also applies to any contracted service providers collecting, using or disclosing personal information on behalf of CMHA-NWV.

Purpose
CMHA-NWV respects and upholds an individual's right to privacy and to the protection of their personal information. We recognize our responsibility to be transparent and accountable in how we use the personal information collected from the people we serve, our employees, volunteers, members, donors and other stakeholders.

In fulfilling our mission to promote the mental health of all, and to support the resilience and recovery of people experiencing mental illness, we sometimes gather and use personal information (as defined in this policy) from employees, clients, members, volunteers and donors. We do this in accordance with British Columbia's *Personal Information Protection Act* (PIPA) which sets out the ground rules for how B.C. businesses and not-for-profit organizations may collect, use and disclose personal information.

This privacy policy, in compliance with PIPA, outlines the principles and practices we will follow in protecting individuals' personal information. Our privacy commitment includes ensuring the accuracy, confidentiality, and security of individuals' personal information and allowing individuals to request access to, and correction of, their personal information. We inform individuals of why and how we collect, use and disclose their personal information; obtain their consent where required; and only handle their personal information in a manner that a reasonable person would consider appropriate in the circumstances.

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. Business contact information is not covered by this policy or PIPA.

"*Individual*" includes clients (any individual receiving services from CMHA-NWV) participants, members, volunteers, employees, and donors.

1. **Collecting Personal Information**

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

- To manage and develop our organization and operations, including personnel and employment matters;
- To manage and develop our volunteer and donor resources;
- To develop, enhance, market or provide products and services;
- To understand the needs and preferences of our clients, volunteers and donors;
- To determine client eligibility for a program, benefit or service;
- To verify identity and enroll a client in a program, benefit or service;
- To advocate on a client's behalf;
- To assist a client with care coordination and/or facilitate integrated service delivery;
- To carry out client file management, as per contract requirements;
- To communicate with clients, members, volunteers, supporters and donors;
- To issue tax receipts;
- To keep members informed and up to date on our activities, special events and opportunities;
- To register individuals for workshops and conferences;
- To contact and thank volunteers and supporters; and
- To meet legal and 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-NWV to collect or 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 an informed 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;
- 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 NWV;
- 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 as 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 or disclose 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 clients 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 client lists or personal information to other parties.

When CMHA-NWV 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.

We may store and process personal information in Canada or another country (e.g. when using a "cloud" based service). In either case, the personal information is protected with appropriate security safeguards, but may be available to government agencies under applicable law.

4. **Releasing Personal Information without Consent**

When it is necessary to release an individual's personal information without consent (because of immediate and severe risk to their or someone else's health, safety, or security), we will keep a written record of what information was released, the person and agency the information was released to, and detailed reasons the release was required.

If the Branch is subpoenaed or a search warrant is executed, the issue of a release of information will be immediately referred to the Privacy Officer or the Executive Director.

In *all* cases where personal information is released without the individual's consent, an Incident Form *must* be completed and sent to the employee's immediate supervisor and the Program Operations Manager as soon as possible and under no circumstance later than *24 hours after the information was released.*

5. **Retaining Personal Information**

If we use an individual's personal information to make a decision that directly affects the individual, we will retain that personal information for *at least one year* so that the individual has a reasonable opportunity to request access to it.

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

6. **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 details of the individual's correction request in the file.

7. **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:

7.1 **Physical Safeguards:**

- Personal information will be stored in locked filing cabinets.
- Employee access to storage areas or filing cabinets will be restricted.
- Files and documents containing personal information will not be left on desks when unattended (e.g., overnight).
- Offices where personal information is held will be physically secured (e.g. locking doors).
- Files containing personal information will not be removed from the CMHA-NWV (e.g. employees will not take files containing personal information home to work on).
- Day timers containing personal information will be secured in a locked briefcase or bag during transport.
- Where files containing personal information need to be transported (e.g. for an office move), a secure courier service should be used.
- Employees must relinquish any personal, privileged, confidential or client information in their possession before or immediately upon termination of employment.

7.2 **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 the CMHA-NWV 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.
- We will ensure that disclosure of personal information or personal health information (whether internally or to a third party) is done with the approval of the Director of Operations or Executive Director.
- When faxes are sent, employees will use a secure faxing service and will follow procedures for ensuring only the authorized recipient has received the fax.

7.3 **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 and USB flash drives will be encrypted.
- Employees shall not load confidential documents onto their unsecured personal computers, smart phones and the public cloud, nor load their own software onto work computers.
- 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, unless encrypted. 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 client initials instead of their full name) and should not provide additional personal information. The receiver may also advise the sender (client 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.

8. **Providing Individuals Access to their 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-client 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 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 or not 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.

9. **Contractors and Service Providers**

This policy applies to all contractors and service providers collecting, using or disclosing personal information on behalf of CMHA-NWV.

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-NWV privacy policy and PIPA. Contracts with service providers will include the Privacy Protection Schedule.

10. **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-NWV
- Requesting clarification where needed; and
- Reporting concerns, complaints and requests for information to the Privacy Officer.

Program Coordinators are responsible for:

- Ensuring compliance with this policy and PIPA in their program; and
- Forwarding any requests for information from clients or participants in their program area to the Privacy Officer to respond.

The Privacy Officer is responsible for:

- Ensuring CMHA-NWV'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;
- Responding to complaints; and
- Liaising with the Office of the Information Privacy Commissioner for BC, where appropriate.

Board Chair, Executive Director and the Director of Operations are responsible for:

- Ensuring there is time and resources for Board members or employees to attend training;
- Supporting Board members or employees in implementing this policy in their area.

11. **Complaints and Requests for Information**

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

Individuals should direct any complaints, concerns or questions regarding CMHA-NWV's compliance, in writing, to the Privacy Officer:

Julia Kaisla
Executive Director
Canadian Mental Health Association-North and West Vancouver
#300-1835 Lonsdale Avenue
North Vancouver, BC V7M 2J8
Mark envelope "Confidential"

If a complaint or request for information is made to CMHA-NWV, 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 by the Privacy Officer.
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 receives a response within 30 business days.
4. If it is a request for information, the requester receives a response within 30 business days.
5. Where applicable, inaccurate or obsolete personal information is corrected or removed and policies and procedures may be modified based on the outcome of the complaint.
6. The date responded and outcome is recorded by the Privacy Officer.
7. All complaints received by the Privacy Officer will be included in an annual report made by the Executive Director to the CMHA-NWV Board of Directors.

If we are not able to resolve the concern, the individual may contact the Office of the Information and Privacy Commissioner for British Columbia:

Office of the Information and Privacy Commissioner for British Columbia
PO Box 9038 Stn Prov. Govt.
Victoria B.C. V8W 9A4
(250) 387-5629.

Callers outside Victoria, call Enquiry BC: 604-660-2421 or toll-free in B.C.:1-800-663-7867 and request a transfer to (250) 387-5629.

info@oipc.bc.ca
www.oipc.bc.ca

12. **Protection of Employees from Reprisal**

No employee shall be disadvantaged or denied any benefit of employment by reason that CMHA-NWV believes that an employee will do anything referred to in paragraphs (a), (b), or (c) below, or by reason that an employee, acting in good faith and on the basis of reasonable belief:

(a) Has disclosed to a Privacy Commissioner that CMHA-NWV or any other person has contravened or intends to contravene a provision of PIPA related to the protection of personal information.

(b) Has refused or stated the intention of refusing to do anything that it is in contravention of a provision of PIPA related to the protection of personal information.

(c) Has done or stated an intention of doing anything that is required to be done in order that a provision of PIPA related to the protection of personal information not be contravened.

13. **Links**

Legislation: Personal Information Protection Act (PIPA)

Implementation Tools for Private Sector Privacy Legislation. Ministry of Technology, Innovation and Citizens' Services

A Guide to PIPA for Businesses and Organizations. (2012) Office of the Information Privacy Commissioner for British Columbia.

Guide to the *Personal Information Protection Act* (for the public). Knowledge and Information Services, Office of the Chief Information Officer, Ministry of Citizen's' Services.

Privacy Protection Schedule

Privacy Helpline
The OCIO also operates a Privacy Helpline, providing support, direction and training to private sector organizations and the public on PIPA's requirements.
Phone: 250-356-1851
Email: Privacy.Helpline@gov.bc.ca