National Operating Policy # 2

Subject: Personal Information and Privacy
Approved: February 23, 2008 by the National Executive Council
Reviewed: May 2021

Objective and Rationale

Privacy of personal information is an important principle to the Canadian Institute of Public Health Inspectors (CIPHI). Canadian Institute of Public Health Inspectors is responsible for the protection of personal information and the fair handling of it at all times, throughout the organization and in dealings with third parties. Care in collecting, using and disclosing personal information is critical to maintaining the confidence of our members and other individuals and groups who have interactions with CIPHI.

Specific Operations

INTRODUCTION AND PERSONAL INFORMATION AND PRIVACY

Organizations covered by the Personal Information Protection and Electronic Documents Act (PIPEDA) must obtain an individual's consent when they collect, use or disclose the individual's personal information. The individual has a right to access personal information held by an organization and to challenge its accuracy, if need be. Personal information can only be used for the purposes for which it was collected. If an organization is going to use it for another purpose, consent must be obtained again. Individuals should also be assured that their information will be protected by specific safeguards, including measures such as locked cabinets, computer passwords or encryption.

PERSONAL INFORMATION

Personal information includes 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 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.

As part of its operations, CIPHI may collect the following personal information from individuals as part of its service delivery:

- First and last name
- Home addresses, telephone numbers, and e-mail addresses
- Date of birth
- Credit card numbers
- Individuals Signatures
- CPHI(C) Certificate #
- Educational background, including transcripts from educational institutions.
- Employment history
- CIPHI administered examination results
- Continuing professional development activities

IDENTIFY THE PURPOSE

CIPHI will identify the reasons for collecting personal information before or at the time of collection. More specifically, CIPHI will:

- Before or when any personal information is collected, identify why it is needed and how it will be used. Document why the information is collected.
- Inform the individual from whom the information is collected why it is needed.
- Identify any new purpose for the information and obtain the individual's consent before using it.

OBTAIN CONSENT

CIPHI will inform members and other individuals in a meaningful way of the purposes for the collection, use or disclosure of personal data. CIPHI will obtain the consent of members, and other individuals before or at the time of collection, as well as when a new use is identified.

LIMITED COLLECTION

CIPHI will not collect personal information indiscriminately and will not deceive or mislead members and others about the reasons for collecting personal information.

LIMITED USE, DISCLOSURE AND RETENTION

CIPHI will use or disclose personal information only for the purpose for which it is collected, unless the individual consents, or the use or disclosure is authorized by legislation.

CIPHI will keep personal information only as long as necessary to satisfy the purposes for which it was collected. This includes personal information used to make a decision about a person for a reasonable time period. This would allow the person to obtain the information after the decision and pursue redress.

Personal information will be retained for a period of 10 years. After this retention period CIPHI will destroy paper files containing personal information by shredding. Electronic information will be destroyed by deleting, and, when the hardware is discarded, CIPHI will ensure that the hard drive

is physically destroyed. Alternatively, CIPHI may send some or the entire file to the applicable member.

STORAGE OF PERSONAL INFORMATION IN THE UNITED STATES*

CIPHI may allow the transfer of personal information held by the corporation to a platform in the United States for storage purposes.

CIPHI is legally permitted to transfer and store personal information in the United States through a third party provided the following requirements are complied with:

- Legislative requirements under PIPEDA and applicable public-sector privacy legislation are met.
- The transfer of information is used solely for storage purposes.
- The use or disclosure of the information by the third party is prohibited unless the express consent has been received from the individual whose personal data is affected.

Provided legal requirements are met the courts, law enforcement, regulators and national security authorities may access personal information stored in the United States.

Prior to entering into an agreement that personal information be stored in the United States CIPHI must demonstrate due diligence by ensuring there are contract terms in place between the parties that:

- support CIPHI privacy policies and comply with legal requirements.
- guarantees confidentiality and security of personal information.
- provide oversight, monitoring and auditing of the service being provided.
- include details of service provider's security policies.

All persons whose data is affected should be notified by CIPHI when the organization enters an agreement to store data in the US and be directed to this policy for further information.

*Reference: Miller Thompson Memorandum March 3, 2021 *"Legal Requirements re: Cross Border Transfer and Storage of Personal Information"*

ACCURACY

CIPHI will minimize the possibility of using incorrect information when making a decision about a member or other individual, or when disclosing information to third parties.

SAFEGUARDS

CIPHI will protect personal information against loss or theft. Personal information will be safeguarded from unauthorized access, disclosure, copying, use or modification. Regardless of the format personal information is in it will be protected.

CIPHI understands the importance of protecting personal information. For that reason, the following steps will be taken:

- Paper information will either be under supervision or secured in a locked or restricted area.
- Electronic hardware is either under supervision or secured in a locked or restricted area at all times. In addition, passwords are used on computers.
- Paper information is transmitted through sealed, addressed envelopes or boxes by reputable companies.
- Electronic information is transmitted either through a direct line or has identifiers removed or is encrypted or password protected.
- Staff and members of the National Executive Council and Board of Certification are aware to collect, use and disclose personal information only as necessary to fulfill their duties and in accordance with our privacy policy.
- External consultants and agencies with access to personal information must have privacy policies and abide by applicable privacy legislation.

OPENNESS

CIPHI will inform members and other individuals about our privacy policies and practices related to the management of personal information. The policies and practices will be accessible on CIPHI's website and will be referenced in CIPHI contracts, membership forms and other CIPHI materials and application forms.

USE OF PERSONAL INFORMATION

When requested, CIPHI will inform members and other individuals if we have any personal information about them. We will explain how it is or has been used and provide a list of any organizations to which it has been disclosed. Members and other individuals will have access to their information. CIPHI will correct or amend any personal information if its accuracy and completeness is found to be deficient or direct the individual on how to correct it themselves if applicable. A copy of the information requested will be provided, unless the legislation allows for the request to be denied. CIPHI will note any disagreement on the file and advise third parties where appropriate.

External Verification of Current Membership Status

The following personal information will be disclosed on National CIPHI website, or upon request, for the purposes of third-party verification of an individual's current membership status:

- CIPHI Branch
- Membership Type
- Preferred name or first name
- Last Name

Updated membership lists will be pulled from the CIPHI Membership Services Centre and post to www.ciphi.ca/membership at a minimum on the following dates April 15, July 15, October 15, and December 31. Information will be displayed alphabetically in the following order: branch, type, last name, and preferred first name or first name.

Upon request from an employer to the appropriate branch president, CIPHI may disclose a list of members within that employer's organization.

Internal Verification of Current Membership Status

As part of routine internal operations CIPHI must utilize personal information to verify the membership status of individual. For the purpose of internal membership verification, the following additional personal information can be accessed by authorized individuals:

- Membership Type
- CPHI(C) Certificate #
- Middle name
- Birth Date

Note: Branches only have access to the personal information of branch members.

For events which require temporary access to membership status has been granted, all electronic and paper copies of the personal information must be destroyed after the event and notification of its destruction communicated national or branch president or an appointed representative.

Internal Communication with Members

As part of routine internal operation CIPHI must communicate directly with its' members. For the purposes of internal communication, the personal information may be shared with authorized individuals:

- First and Surname
- Home Address
- Home Phone #
- Home Email Address
- Work Address
- Work Phone #
- Work Email Address

Note: Branches only have access to the personal information of branch members.

Before personal information is accessed by authorized individual the method and content of the communication must be approved by the national or branch president or an appointed representative.

Volunteer consent for disclosure of personal information

As part of the membership renewal process individuals are asked to provide consent for CIPHI to release personal information for the purposes of fundraising and/or to Corporate/Affiliated members for the purpose of advertising. For those members that provide consent to the disclosure of their personal information the following can be provided:

- First and Surname
- Home Address (street address, City, Province, and Postal Code)

Before access to this personal information is granted the requesting party must provide written a request to national office outlining use of the information, a copy of their personal information privacy policy, and who will have access to the information.

The National Executive Council or a appoint representative will review the request and approve the release of the personal information.

As the consent for voluntary disclosure of personal information for fundraising and advertising occurs annually, requesting parties can only use the information for current membership year. All electronic and paper copies must be destroyed by the end of the request membership year and notification of its destruction sent to the national president or an appointed representative.

RECOURSE

A member of the National Executive Council should be contacted to address any questions or concerns you might have. If you wish to make a formal complaint about our privacy practices, you may make it in writing to the National President. They will acknowledge receipt of your complaint; ensure that it is investigated promptly and that you are provided with a formal written decision with reasons.

Accountability
CIPHI has appointed the National Executive Council to be responsible for CIPHI's compliance with privacy legislation. CIPHI will protect all personal information which it holds or is transferred to a third party for processing.

Attachments / Appendices

Document Change History
Revised May 2021 – *Storage of Personal Information in US*