AMHSA
Health | Safety | Environment

Created: 13 June 2023
Save Date: 13 June 2023
Print Date: 13 June 2023

Revision	Prepared By	Date Prepared
0.1	Krystal Mc Dowell, Scott Lyall, Jessica Meyer	04/06/2022
Effective Date	**Reviewed By**	**Date Reviewed**
5/30/2023	Olana Todoruk, Craig Hrynchuk, PrivacyWorks	

Privacy Policy

Scheduled Review Date: June 2026

Policy Statement

The Alberta Municipal Health and Safety Association (AMHSA) is an organization committed to protecting the personal information of our members and others who engage with AMHSA. We support a general policy of openness about how we collect, use, disclose and protect the personal information of our members.

As a non-profit organization established in Alberta, we comply with Alberta's Personal Information Protection Act. It is AMHSA's intent to also comply with privacy legislation within each jurisdiction in which AMHSA operates across Canada.

Purpose

This Policy acts as the articulation of AMHSA's privacy practices and standards about the collection, use and disclosure of personal information and personal employee information in the course of its business activities.

This Policy also describes how an individual can contact AMHSA if they have questions about AMHSA's privacy practices or would like to request to access or correct their personal information.

Scope

This Policy applies to all personal information and personal employee information that are collected, used, and disclosed by AMHSA when providing its services and performing its business activities that are subject to the provisions of Canada's federal and provincial privacy laws, as applicable.

This Policy applies to all employees, volunteers, members, learners, third parties or other individuals and organizations contracted by AMHSA and is intended to guide all actions performed by those individuals when accessing, using and disclosing information.

Responsibilities

Board of Directors

- Understanding and overseeing the management of principal risks to AMHSA's business, including AMHSA's privacy program.

Executive Director

- Approve and implement policies that support escalation and reporting of validated privacy breach incidents to the AMHSA board of directors executive;
- Privacy breach reporting to the Board of Directors and Privacy Commissioner as required
- Compliance with privacy laws;
- Communications with provincial and federal privacy commissioners, and other governmental authorities responsible for privacy; and
- Investigations, inquiries, complaints, and other proceedings related to the privacy of personal information.

Privacy Officer

- Responding to requests for access to, and correction of, personal information, and other requests from data subjects;
- Facilitate inquiries, complaints, Investigations and other proceedings related to the privacy of personal information; and
- Privacy breach response and reporting (If applicable).

Director of Corporate Services

- Oversight of collection, use, and disclosure of personal information;
- Investigations of potential IT breaches as required;
- Departmental any systems compliance with privacy laws;
- Ensuring all employees receive appropriate personal information privacy training;
- Ensuring personal information is stored and transmitted according to AMHSA's data classification system; and
- Ensuring personal information is stored and transmitted according to AMHSA's data classification system (further information about AMHSA's data classification system is available in the IT/Cyber Security and Data Breaches Policy).

Director of Learning and Assurance

- Investigations, inquiries, complaints, and other proceedings related to the privacy of personal information;
- Departmental any systems compliance with privacy laws;
- Privacy breach response and reporting; and
- Ensuring all employees receive appropriate personal information privacy training.

Projects and Marketing Coordinator

- Meet requirements for CASL (Canadian Anti-Spam Legislation)
- Treat the use of email addresses for communications with adherence to this policy.

Employees

- Ensuring that personal information is collected, used, and disclosed in accordance with this Privacy Policy and as otherwise directed by AMHSA;
- Ensuring personal information is collected, used, and disclosed on a need-to-know basis, and only for the purposes of carrying out the employee's roles and responsibilities to AMHSA;

- Acknowledging and signing AMHSA's privacy and security policies on an annual basis;
- Attending all personal information privacy and security training assigned by Functional Leader;
- Diligently reporting any actual or suspected improper collection, use, or disclosure of personal information; and
- Diligently safeguarding the confidentiality and privacy of personal information, including by maintaining a clean desk at all times; not leaving sensitive or confidential information, including personal information, unattended; and securely transferring physical and electronic records.

Contractors

- Ensuring that personal information is collected, used, and disclosed in accordance with this policy and as otherwise directed by AMHSA;
- Diligently reporting any actual or suspected improper collection, use, or disclosure of personal information; and
- Diligently safeguarding the confidentiality and privacy of personal information, including always maintaining a clean desk; not leaving sensitive or confidential information, including personal information, unattended; and securely transferring physical and electronic records.

Collecting Personal Information

AMHSA collects and maintains different types of personal information in respect of the individuals with whom we interact.

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

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

- To obtain a membership;
- To establish, maintain and manage client relationships and provide products and services that have been requested;
- To provide the opportunity for client's to review the products and services that AMHSA provides;
- To comply with an individual's requests and deliver the requested services;
- To enroll, open and manage accounts for leaners to access courses offered by AMHSA through AMHSA's Learning Management System (LMS);
- To maintain the integrity of the courses offered to clients and to be able to provide records related to such courses;
- To protect AMHSA against error, fraud, theft and damage to our goods and property;
- To comply with applicable law or regulatory requirements;
- To manage and maintain employees relationships; and
- Any other purpose to which an individual consents.

Consent

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

Consent can be provided orally, in writing, or electronically, 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 his or her personal information being used for activities such as mail-outs, 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 to the 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 AMHSA's ability to provide a particular service or product. If so, AMHSA will explain the situation to assist the individual in making the decision.

AMHSA may collect, use, or disclose personal information without the individual's knowledge or consent only in specific situations as authorized by law, including:

- In an emergency that threatens an individual's life, health, or personal security;
- When the personal information is available from a public source (e.g., a telephone directory);
- When AMHSA requires legal advice from a lawyer;
- To protect AMHSA from fraud; and
- To investigate an anticipated breach of an agreement or a contravention of law.

Consent may be changed or withdrawn by an individual at any time, subject to legal or contractual obligations and reasonable notice.

Using and Disclosing Personal Information

AMHSA will only use or disclose personal information where necessary to fulfill the purposes identified at the time of collection as outlined in the section *Collecting Personal Information* above, except as authorized by law.

AMHSA may use or disclose personal information for the following purposes:

- As permitted or required by applicable law or regulatory requirements;
- To comply with valid legal processes such as search warrants, subpoenas or court orders;
- As part of AMHSA's regular reporting activities to regulatory bodies;
- To provide an individual records relating to courses, including course completion certificates generated by the LMS;
- To conduct surveys in order to enhance the provision of our services;
- To contact individuals directly about products and services that may be of interest;

- In the case of a prospective, current, or former employee of a municipality or other public body, AMHSA may disclose information related to the courses an individual has taken to the municipality or public body;
- To assist AMHSA with relationship management activities;
- To protect the rights and property of AMHSA;
- During emergency situations or where necessary to protect the safety of a person or group of persons;
- Where the personal information is publicly available; or
- With an individual's consent (e.g., were individuals wish to share contact information so they can stay in touch with their fellow learners of the same course. In such situation, consent to share one's name, email address, and other personal information with other members of the same course will be sought).

AMHSA will not use or disclose personal information for any additional purpose unless AMHSA obtains consent to do so.

AMHSA will limit access to personal information, integrating the principles of least privilege and need-to-know into its business activities. As such, personal information may only be used or disclosed within the limits of each employee's role. Employees may not read, look at, receive or otherwise use or disclose personal information unless they have a legitimate need-to-know as part of their position.

Sharing and Disclosure of Personal Information to Third Parties

AMHSA may disclose personal information to third parties, including: third parties that provide services to AMHSA or on AMHSA's behalf; third parties that assist AMHSA in the provision of services to individuals; and third parties whose services AMHSA uses to conduct business.

AMHSA will endeavor to retain personal information within Canada; however, where disclosure to third-parties outside of Canada is necessary, AMHSA will work towards trusted and secure locations and providers. For example, AMHSA' utilizes *Civilized Discourse*, with servers located in USA, *Constant Contact*, with servers located in USA but with personal data processed outside of USA. All these parties may provide certain information technology and data processing services to AMHSA from time to time so that AMHSA may conduct its business activities, and as result, personal information may be collected, used, processed, stored or disclosed in Canada, the United States of America, or elsewhere.

Personal information may be disclosed or transferred to another party during the course of, or completion of, a change in ownership of or the grant of a security interest in, all or a part of AMHSA through, for example, an asset or share sale, or some other form of business combination, merger or joint venture. In such a case, AMHSA will provide that such party is bound by appropriate agreements or obligations and required to use or disclose personal information in a manner consistent with the use and disclosure provisions of this Policy, unless an individual consents to otherwise.

AMHSA Events

During in-person and online events, photographs may be taken and the events may be recorded. Photographs, including biographies, may be published in various media, including print and online, without further notice.

AMHSA, our partners and event attendees may also post discussions, pictures and biographies on various social media channels. We also regularly host events that operate under a modified Chatham House Rule – that is that contributions may be published but are not to be attributed to any individual speaker. Invitations to such events will explicitly state that the event is operating under such restrictions, however AMHSA is not responsible for personal information posted by event participants.

AMHSA Learning Management System (LMS)

For the purposes of the LMS, all AMHSA employees will be granted access privileges to input required learner information into the LMS, generate course completion certificates (where automated certificates are not generated), and improve education and training content.

Where contracted instructors are facilitating a course, access privileges to the LMS will be limited to profiles of learners enrolled in the course to input exam marks and confirmation of course completion. Where a course completion certificate is not automatically generated, the contracted instructor will be permitted to manually generate certificates for learners within their assigned courses. AMHSA will immediately revoke the contracted instructor's access to the LMS upon dissolution of the contracting agreement.

A supervisor and/or manager of a learner may be granted access to learner information for learners who report to them within their organization. Confirmation of course completion may be released to supervisors and/or managers upon request for the learners that report to them after validation of consent or notice (where applicable) provided by the organization to AMHSA.

Anonymized Data

AMHSA uses third-party platforms to gather and analyze information related to business activities to better understand opportunities to enhance service offerings, learner/client experiences, and interactions. Information may be collected passively (e.g., monitoring time spent on one of our web pages) or actively (e.g., circulating a survey to learners). AMHSA only uses anonymized information collected via the third-party platforms to inform our analysis and decision-making.

Personal Employee Information

In addition to legal requirements for personal information, specific requirements are set out in legislation for personal employee information. Personal employee information is personal information about an employee or volunteer which is collected, used or disclosed solely for the purposes of establishing, managing or terminating an employment relationship or a volunteer work relationship.

The subsections in Section 8 refer specifically to the collection, use and disclosure of personal employee information. For other privacy requirements concerning personal employee information,

such as data retention, accuracy, access, security that are outlined in this Policy, AMHSA will provide the same level of protection and controls to personal employee information as it does to personal information.

Collection of Personal Employee Information

AMHSA will collect different types of information in respect of employees (including current, prospective, and former employees and volunteers), including personal information contained in:

- Resumes and/or applications;
- References and interview notes;
- Photographs and videos;
- Offer letters and employment contracts;
- Criminal background checks, including police information checks and vulnerable sector checks, as applicable;
- Vaccination records;
- Policy acknowledgement forms;
- Payroll information, such as social insurance numbers and pay cheque deposit information;
- Wage and benefit information;
- Forms relating to the application for or changes to employee health and welfare benefits, including, short and long term disability, life insurance, optional life insurance, accidental death & dismemberment, medical and dental care; and
- Beneficiary and emergency contact information.

In addition to the information contained above, AMHSA may also collect identification information such as name, home address, telephone, personal email address, date of birth, employee identification number and marital status, specific medical information that an employee provides to AMHSA and any other information that is voluntarily disclosed by the employee.

Use and Disclosure of Personal Employee Information

The personal employee information collected is used and disclosed to establish, manage or terminate an employment relationship with AMHSA. Such uses include:

- Determining eligibility for initial employment, including the verification of references and qualifications;
- Administering pay and benefits;
- Processing employee work-related claims (e.g. workers' compensation or insurance claims);
- Establishing training and/or development requirements;
- Conducting performance reviews and determining performance requirements;
- Assessing qualifications for a particular job or task;
- Establishing a contact point in the event of an emergency (such as next of kin);
- Complying with applicable labour or employment statutes;
- Compiling directories and telephone lists;
- Ensuring the security of AMHSA-held information; and
- Other purposes as reasonably required by AMHSA to establish, manage or terminate an employment relationship.

AMHSA may share personal employee information with members, employees, contractors, consultants and other parties who require such information to assist AMHSA with employee relationship management activities. Payroll and benefits service providers may provide certain information technology and data processing services inside Canada, but outside of Alberta, to AMHSA from time to time so that AMHSA may conduct its business activities.

As a result, personal employee information may be collected, used, processed, stored or disclosed in the United States of America or other jurisdictions. In these circumstances, the governments, courts, law enforcement, or regulatory agencies of such other jurisdictions may be able to obtain access to personal employee information through the laws of the foreign country.

Notice and Consent

AMHSA may collect, use, and disclose personal employee information without consent for the purposes of establishing, managing or terminating the employment relationship.

AMHSA will provide current employees with prior notice about what information AMHSA collects, uses or discloses and the purpose for doing so.

AMHSA will inform employees of any new purpose for which AMHSA will collect, use, or disclose personal employee information, or will obtain the employee's consent, before or at the time the information is collected.

Where consent is required for collection, use or disclosure of personal employee information, the employee may, at any time, subject to legal or contractual restrictions and reasonable notice, withdraw consent. All communications with respect to such withdrawal or variation of consent should be in writing and addressed to the AMHSA Privacy Officer.

Employee References

Where AMHSA is contacted by other organizations and asked to provide a reference for an individual, it is AMHSA policy not to disclose personal information about employees and volunteers to other organizations who request references without consent. The personal information we normally provide in a reference includes:

- Confirmation that an individual was an employee or volunteer, including the position, and date range of the employment or volunteering.
- General information about an individual's job duties and information about the employee or volunteer's ability to perform job duties and success in the employment or volunteer relationship.

Retaining Personal Information

AMHSA will retain personal information only as long as necessary to fulfill the identified purposes or as required by law.

AMHSA will securely destroy or render the information anonymous where no legitimate purpose exists to justify the retention of the personal information or as required by law.

AMHSA will adhere to best practices for the destruction of electronic and physical information, including back-ups, as updated from time to time.

AMHSA Learning Management System

AMHSA maintains learner training records originally collected in the LMS indefinitely.

Where a learner would like to request removal of their personal information or the full training record, the learner may request such removal via email to safety@amhsa.net. AMHSA will render the requested information and/or record(s) inaccessible within 48 -hours. Access to the archival system is limited to authorized AMHSA employees.

In cases where a learner is no longer employed with a municipality or organization transacting with AMHSA, AMHSA will work with all parties involved (previous employer, current employer, learner) to ensure privacy and confidentiality of personal information is maintained.

Ensuring Accuracy of Personal Information

AMHSA 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.

A request to correct personal information should be forwarded to AMHSA's Privacy Officer. If the personal information is demonstrated to be inaccurate or incomplete, AMHSA will correct the information as required and send the corrected information to any organization to which AMHSA disclosed the personal information in the previous year. If the correction is not made, AMHSA will note the clients', customers', members' correction request in the file.

Securing Personal Information

AMHSA endeavors to maintain physical, technical, and procedural safeguards that are appropriate to the sensitivity of the personal information in question. These safeguards are designed to prevent personal information from loss and unauthorized access, copying, use, modification, or disclosure.

AMHSA will apply the following security measures to ensure that personal information and personal employee information is appropriately protected, including without limitation:

- The use of locked filing cabinets;
- Physically securing offices where personal information is held;
- The use of user IDs, passwords, encryption, firewalls; and
- Restricting employee access to personal information as appropriate (i.e., only those that need to know will have access; contractually requiring any service providers to provide comparable security measures).

AMHSA will use appropriate security measures when destroying personal information and personal employee information including physically shredding documents and permanently deleting electronically stored information.

AMHSA will continually review and update security policies and controls as technology changes to ensure ongoing personal information security for all of AMHSA's infrastructure including the Learning Management System.

Physical Transportation of Personal Information

Where physically transporting personal information, including in electronic form (such as on laptops or USB drives) or hard copy, such information must be secured in a closed, opaque container (e.g., a briefcase) marked as "CONFIDENTIAL" and marked with AMHSA contact information (e.g., name, business address, and telephone number). During transport, the data container must be under the direct control of employee(s) throughout the travel period.

Where using a privately owned vehicle (including rental car) to transport personal information, the employee(s) must secure all information in the vehicle's trunk (or equivalent) during transport; the information cannot be visible or left unattended.

Employees are solely responsible for security and control of the container and data while off-duty. Off site, including at home, storage of personal information must be stored according to AMHSA's data classification system. Personal information stored offsite must be in a locked filing cabinet.

Access to Personal Information

Individuals have a right to access their own personal information in a record that is in the custody or under the control of AMHSA, subject to some exceptions. For example, organizations are required under the Alberta's PIPA to refuse to provide access to information that would reveal personal information about another individual.

A request for access can be made by writing to the Privacy Officer, who is designated to ensure compliance with PIPA and other provincial and federal legislation (see contact details below in the Accountability section)

The individual must provide sufficient information in the request to allow AMHSA to identify the information the individual is seeking. The individual may also request information about AMHSA's use of the personal information and any disclosure of that information to persons outside the organization. The individual may request a correction of an error or omission in their personal information.

If AMHSA refuses a request in whole or in part, AMHSA will provide the reasons for the refusal. In some cases where exceptions to access apply, AMHSA may withhold that information and provide the individual with the remainder of the record.

AMHSA will respond to requests within 45-calendar days, unless an extension is granted.

AMHSA may charge a reasonable fee to provide information, but not to make a correction. AMHSA will not charge fees when the request is for personal employee information.

AMHA will advise the individual of any fees that may apply before beginning to process the request.

Privacy Breaches

All confirmed or suspected privacy breaches must be reported immediately to the Privacy Office, which will execute the *IT/Cyber Security and Data Breaches Policy*.

AMHSA's Privacy Officer will oversee all privacy breach management steps including, containing the breach, evaluating risks associated with the breach, breach notification, reporting, and prevention.

AMHSA must notify the Alberta Information and Privacy Commissioner (or respective Commissioner if the personal information is governed under other provincial and federal legislation) if an incident occurs involving loss of or unauthorized access to or disclosure of personal information that may pose a real risk of significant harm to individuals.

Accountability

AMHSA have appointed a Privacy Officer to oversee compliance with this Privacy Policy. The contact information for the Privacy Officer is as follows:

Privacy Officer
Attn: Craig Hrynchuk
Phone: 1-800-267-9764
Address: 176, 2755 Broadmoor Blvd, Sherwood Park AB, T8H 2W7
E-mail: privacyofficer@amhsa.net

In addition, the following roles are accountable for maintaining compliance with PIPA and all privacy-related policies:

Compliance with Canada's Anti-Spam Legislation (CASL)

AMHSA must comply with Canada's Anti-Spam Legislation (CASL). Each electronic communication will include an opt-out feature and instructions on how to un-subscribe if individuals no longer wish to receive future e-mails from AMHSA. If individuals do not expressly consent to receiving electronic communications, AMHSA will only communicate with them for the limited purposes permitted under CASL.

Revisions to this Privacy Policy

From time to time, AMHSA may make changes to this Policy to reflect changes in its legal or regulatory obligations or the manner in which AMHSA handles personal information. AMHSA will make available the revised version of this Policy.

Interpretation of this Privacy Policy

Any interpretation associated with this Policy will be made by the AMHSA Privacy Officer. This Policy includes examples but is not intended to be restricted in its application to such examples, therefore where the word "including" is used, it shall mean "including without limitation."

This Policy does not impose upon AMHSA any obligations, or create or confer upon any individual any rights, outside of, or in addition to, those imposed by Canada's federal and provincial privacy laws, as applicable. Should there be, in a specific case, any inconsistency between this Policy and Canada's federal and provincial privacy laws, as applicable, this Policy shall be interpreted, in respect of that case, to give effect to, and comply with, such privacy laws.

Definitions

For the purposes of this Policy, the following terms will apply as defined by Alberta's *Personal Information Protection Act* (PIPA):

Anonymized Data: means a type of data that has been processed to remove personally identifiable information to protect the privacy of individuals while still allowing for meaningful analysis. This type of data is often used in research, analytics, and other data-driven activities.

Business Contact Information: means a type of data that has been processed to remove personally identifiable information to protect the privacy of individuals while still allowing for meaningful analysis. This type of data is often used in research, analytics, and other data-driven activities..

Employee: means an individual employed by the organization and includes an individual who performs a service for or in relation to or in connection with an organization (i) as a partner or a director, officer, or other office-holder of the organization (i.1) as an apprentice, volunteer, participant or student, or (ii) under a contract or an agency relationship with the organization. or provides a service for the organization, including an apprentice, volunteer, cooperative student, an individual (not a company) acting as a contractor or agent for the organization.

Functional Leader: is both a positional role (when required for organizational accountability and responsibility) and a leadership style dedicated to determining what actions and behaviors establish effective leadership and sharing that information with all interested parties - rather than empowering a single person to lead.

Learning Management System (LMS): means a software application for the administration, documentation, tracking, reporting, automation, and delivery of educational courses, training programs, materials or learning and development programs.

Personal Employee Information: means in respect of an individual who is potential, current or former employee of an organization, personal information reasonably required by the organization for the purposes of (i) establishing, managing or terminating an employment or volunteer-work relationship, or (ii) managing a post-employment or post-volunteer-work relationship between the organization and the individual, but does not include personal information about the individual that is unrelated to that relationship.

Personal Information: means any information about an identifiable individual and may include, but not limited to, name, address, age, gender, contact information, employment history, payment details and education status. It does not include business contact information or anonymized data.

Related Documents

IT/Cyber Security and Data Breaches Policy
File Retention Policy
Electronic Communication
Use of Software
Information Technology Administration and Purchasing
Mobile Device

Craig Hrynchuk
_____
Craig Hrynchuk, Executive Director

June 6, 2023
_____
Date