Policies and Standard Operating Procedures
Version 2.0

Calgary Homeless Foundation

308-925 7 Avenue South West
Calgary, AB T2P 1A5, Canada

Effective Date
July 25, 2016

Table of Contents

Section 1.0 Introduction and Definitions

1.1. Introduction

The Calgary Homeless Management Information System (HMIS) is a web based, electronic Client management information system providing a standardized assessment of Client needs, individualized service plans and service records. The Calgary community utilizes the HMIS to understand the nature of homelessness, develop policies and initiatives to address homelessness, and coordinate case management services. The Calgary HMIS is a product of Bowman Systems' ServicePoint™ and managed by the HMIS Team at the Calgary Homeless Foundation (CHF).

As the recipient of conditional grant funding from both provincial and federal government bodies, CHF is deemed to be a government "employee" under the *Freedom of Information and Protection of Privacy Act* (FOIP). As such, CHF's personal information collection, use and disclosure activities and the use of HMIS to manage this information are subject to the protection of personal information provisions of FOIP. In addition, FOIP governs all HMIS data that are provided by agencies that are funded in whole or in part by FOIP public bodies, whether that funding is direct or through the CHF.

The Calgary Homeless Foundation, in consultation with the historical HMIS Advisory Committee, established the original Policies and Standard Operating Procedures in 2012. This document is now owned, reviewed and updated annually by the HMIS Team. This document still continues to guide HMIS use and continues to set forth the requirements of accountability, continuity, and compliance. As set out in Sub-Section 1.3 of this document, the HMIS Team will be continually reviewing and updating the Policies and Standard Operating Procedures document as required to ensure ongoing viability and responsiveness.

The Policies and Standard Operating Procedures provides guidelines, requirements, responsibilities, processes, and procedures governing the operation of the HMIS.

1.2. Definitions

The following is a list of terms and acronyms found in this document along with their definitions.

Analysis: Reviewing, organizing and interpreting data from the HMIS into useful information.

Authorized User: Any individual who uses a particular software package; in this case, Bowman Systems ServicePoint™.

Bowman Systems: HMIS software vendor.

Calgary Homeless Foundation (CHF): The agency that maintains and oversees the operation of the HMIS system.

Client: An individual who is a recipient of services offered by a Participating Agency at any time and from whom Personal Information may be collected.

Client-level Data: Data collected or maintained about a specific person. This type of data can be de-identified for purposes of data analysis, which means that personally identifying information is removed from the record.

Control: Refers to the authority of an Agency to manage a record, including restricting, regulating and administering its use, disclosure or disposition.

Custody: Refers to the physical possession of a record.

Data Element: A basic unit of information built on standard structures having a unique meaning and distinct units or values.

Data-mining: A process of scanning data in the HMIS for the purpose of discovering patterns and developing data sets for analysis and reporting.

De-identified Data: The removal of any personally identifying information from the HMIS such that the Client record shall no longer be able to be reasonably retraced to a specific individual.

Dissemination: Any release of HMIS data by the CHF, a Participating Agency, or an authorized User.

Firewall: A method of controlling access to a private network in order to provide security of data. Firewalls can use software, hardware, or a combination of both to control access.

FOIP: The *Freedom of Information and Protection of Privacy Act*. This Act sets out the rules for collection, use or disclosure of personal information by public bodies.

HIA: The *Health Information Act.* This Act sets out the rules regarding collection, use and disclosure of personal health information.

HMIS: The specific Homelessness Management Information System utilized by the CHF.

HMIS Advisory Group: A group made up of community members, experts and advice givers that is convened at times when guidance and direction are required on initiatives that affect the whole community.

HMIS Agency Administrator: The person(s) responsible for HMIS oversight at the Agency.

HMIS Team: The individuals at the CHF, who manage daily HMIS operations, develop and maintain HMIS resources and provide HMIS system support to HMIS Users. These individuals have access to all User and administrative functions and Client records.

HMIS Server: A computer housed in Canada on a Canadian network that manages HMIS resources for use by other computers in the network. For example, a file server stores files that other computers (with appropriate permissions) can access. One file server can "serve" many files to many computers. A database server stores a data file and performs database queries for computers.

HMIS Uses and Disclosures: The uses and disclosures of Personal Protected Information that are allowed by these standards.

HPS: Homelessness Partnering Strategy.

HS: Government of Alberta Human Services.

Participating Agency: Any agency, organization or group who has an HMIS Participating Agency Agreement with the CHF and that is allowed access to the HMIS database. These agencies connect independently to the database via the Internet.

Participating Agency Agreement: An agreement outlining terms of use and service between an agency using HMIS and the Calgary Homeless Foundation.

Personally Identifying Information: Information that is unique to an individual and that may be used to identify a specific person. Examples of identifying information are name and Provincial Health Number.

Personal Information: Any recorded information about an identifiable individual as defined in the *Freedom of Information and Protection of Privacy Act*, s1(n).

Personal Protected Information (PPI): Any information maintained by or for an Agency about a living Client or individual that: (1) identifies, either directly or indirectly, a specific individual; (2) can be manipulated by a reasonably foreseeable method to identify a specific individual; or (3) can be linked with other available information to identify a specific individual.

PIPA: The *Personal Information Protection Act*. This Act sets out guidelines surrounding the collection, use and disclosure of personal information by private sector and certain non-profit organizations.

Program Data Elements (PDE): Questions that are specifically designed to gather information that relates to a specific program or program type.

Research and Development (RAD) Director: The person responsible for HMIS oversight at the CHF.

ROI: Release of Information.

ServicePoint™: The web-based database software developed by Bowman Systems that is used within HMIS.

Universal Data Elements (UDE): Questions that are designed to obtain broad demographical information

User License: A license (usually purchased) that allows an individual to use a specific product or service. In this case, the license pertains to Bowman Systems' ServicePoint™. User licenses cannot be shared.

Vendor: A company that supplies a specific product or service. In this case, Bowman Systems is the HMIS vendor.

1.3. Policies and Standard Operating Procedures Revision Schedule

This document shall be reviewed at least once per annum by the HMIS Team. Any changes that are required shall be made at this time, although the HMIS Team reserves the right to update this document on an ongoing basis as required.

Section 2.0 Stakeholders

2.1. The Calgary Homeless Foundation

Purpose: To define the role and responsibilities of the CHF as they relate to the Calgary HMIS Initiative.

Policy: The CHF will hire and assign staff to implement, operate, maintain, and monitor the HMIS.

Responsibilities: To enter into and provide oversight on, contractual agreements with funders, Participating Agencies, consultants, researchers, and the HMIS Vendor.

The CHF shall:

- Act as central point of communication between the HMIS Advisory Group and Participating Agencies;

- Provide stewardship and make positive use of the information entrusted to the CHF on behalf of the community;

- Convene and coordinate the HMIS Advisory Group, HMIS Users Group, and other meetings with HMIS Stakeholders as required;

- Supervise the contractual relationship between the CHF and the HMIS Vendor;

- Provide guidance, technical infrastructure, and support to successfully operate the HMIS;

- Ensure the data collected within the HMIS is FOIP compliant.

- Monitor data quality within the HMIS.

- Mine, analyze, and report HMIS data to respond to requests for information from Participating Agencies, Funders, and other community Stakeholders in compliance with Section 4.0 of this document.

2.2. HMIS Advisory Group

Purpose: To define the roles and responsibilities of the HMIS Advisory Group.

Policy: When required, the HMIS Advisory Group will provide guidance and recommendations to HMIS Team, which is responsible for implementing, operating and maintaining the HMIS.

Responsibilities: The HMIS Advisory Group will be convened on an "as needed" basis to make recommendations to HMIS Team on selected issues pertaining to the operation and/or any substantial changes to the HMIS system. The HMIS Team will take into strong consideration the Advisory Group's advice in all decisions as they relate to HMIS.

2.3. Calgary HMIS Team (Manager and Staff)

Purpose: To define the roles and responsibilities of the HMIS Team (Manager and Staff)

Policy: The CHF will provide a team of individuals to oversee day-to-day HMIS operations and monitoring, establishing the HMIS Team.

Responsibilities:

- **Daily Operation:**

    - Manage contractual agreements between the CHF and Participating Agencies;

    - Provide guidance to Participating Agencies on implementing and maintaining the HMIS Policies and Standard Operating Procedures as needed;

    - Auditing access to and use of HMIS to document full participation and compliance by Participating Agencies;

    - Monitor data quality with regard to accuracy, timeliness and completeness and notify agencies if problems arise;

    - Conduct data quality assessments each quarter at minimum;

    - Conduct annual onsite data quality and HMIS Policies and Standard Operating Procedures review at participating agencies;

    - Store and maintain all HMIS-related files, records and documents;

    - Audit HMIS Policies and Standard Operating Procedures compliance;

    - Develop and generate reports for the CHF and Participating Agencies in compliance with the HMIS Policies and Standard Operating Procedures; and

    - Review and update the HMIS Policies and Standard Operating Procedures as required or at minimum once per annum.

- **Develop and Manage Resources**

  - Research, interpret and prepare information for grant applications and other funding sources as needed;

  - Support the submission and coordination of proposals and grant applications with participating agencies and representatives;

  - Manage activities to ensure compliance with funding requirements, regulations and policies; and

  - Ensure that relevant components of the 10-Year Plan to End Homelessness are integrated into the HMIS structure.

- **System Support:**

  - Provide ongoing training on data entry, reporting, privacy practices and security requirements;

  - Provide basic user training to new HMIS users as required;

  - Provide Participating Agencies with assistance to support their successful use of HMIS, including on-site support;

  - Operate a help-desk during normal business hours and respond to all inquiries in a timely manner in accordance with the Participating Agency Agreement;

  - Conduct HMIS User Group meetings to discuss HMIS updates, data quality, reports and system use issues;

  - Manage the HMIS User interface to enhance usability for Participating Agencies;

  - Coordinate and assist in data migration and ongoing data sharing with external data systems;

  - Issue software user licenses, grant access to authorized users, and reset User passwords as required;

  - Manage software version updates and standardized notifications process to all Participating Agencies;

  - Monitor issues related to contractual performance of the HMIS software vendor pertaining to software development, system upgrades, hosting and data protection services;

  - Monitor technical aspects of system functioning, speed, and database back-up procedures of the HMIS; and

  - Monitor issues related to privacy, including conducting and reviewing Privacy Impact Assessments as required.

2.4. Participating Agency

Purpose: To define the roles and responsibilities of the Participating Agency.

Policy: A Participating Agency using the HMIS will oversee their Agency staff's usage of the HMIS and compliance to the HMIS Policies and Standard Operating Procedures.

Responsibilities:

- Sign the required HMIS Participating Agency Agreement, as set out in Appendix "A", indicating a commitment to implement and adhere to all Policies and Standard Operating Procedures set forth;

- Designate an HMIS Agency Administrator to represent the Participating Agency at HMIS meetings and manage the Participating Agency's use of HMIS;

- Participate in the HMIS Users Group when required;

- Only request user licenses at a security level, as set out in Appendix "F", that allows no more access to information than needed to perform job responsibilities;

- Ensure Authorized Users who require access to the HMIS in relation to job duties have proficient skills to use a web-based Client management information system;

- Establish and maintain a confidentiality policy that includes procedures related to Client confidentiality, staff misconduct, and violations;

- Establish Agency protocols and practices that adhere to the HMIS Policies and Standard Operating Procedures (CHF may provide guidance and sample language if needed);

- Maintain Agency computer hardware and Internet connectivity;

- Apply security measures as outlined in the Security Policy to all the systems where confidential Client data is stored, including, but not limited to an Agency's networks, desktops, laptops, mini-computers, tablets, cellphones, mainframes, and servers (CHF can provide guidance on meeting this policy);

- Ensure the Agency has adequate technical support to successfully access the Internet and comply with all system and security requirements as set out in sections 3.2 and 5.10 of this document;

- Encourage and monitor data quality;

- Comply with the CHF's HMIS Privacy and Security measures as outlined in the Calgary Privacy Impact Assessment and monitor ethical data collection and maintenance;

- Establish an Agency procedure to accept and consider all Client requests to view and correct his/her information maintained in the HMIS;

- Comply with HMIS Grievance Procedure to accept and submit all Client grievances about the HMIS Privacy and Security Policies and Practices to the HMIS Team;

- Comply with necessary data collection in compliance with the HMIS Policies and Standard Operating Procedures;

- Require each member of the Agency's staff (including employees, volunteers, affiliates, students, contractors, and associates) who require access the HMIS to attend an HMIS User Training session and sign an HMIS User Agreement that acknowledges receipt of a copy of the HMIS Policies and Standard Operating Procedures and that pledges to comply with the HMIS Policies and Standard Operating Procedures before accessing the HMIS;

- Secure any paper or other hard copy containing Personal Protected Information (PPI) that is either generated by or for HMIS, including, but not limited to assessments, reports, data entry forms, signed HMIS Release of Information (ROI) forms; and

- Review and comply with the HMIS Electronic Data Collection Policy

2.5. HMIS Agency Administrator

Purpose: To define the roles and responsibilities of the HMIS Agency Administrator.

Policy: Participating Agencies will provide a single point of contact (or multiple if Agency site is large) for all HMIS communication and coordination. The Agency Administrator will also complete the Agency Administrator training, (in addition to the Basic HMIS User training), and complete and submit an Agency Admin User Agreement, as set out in Appendix "B".

Responsibilities:

- Coordinate with the HMIS Team a time to receive the advanced Agency Admin training;

- Provide a single point of communication between the CHF and Authorized Users and disseminate information received to all Agency staff on the HMIS;

- Make requests for interface changes and field additions to the HMIS Team for approval and prioritization;

- Ensure the Agency collects and maintains UDEs and, as appropriate, Funder Assessments;

- Ensure a representative from the Agency attends the HMIS Users Group meetings and disseminates learnings to other Agency staff.

- Ensure Agency staff with access to the HMIS have attended training and have signed the HMIS User Agreement;

- Assist Authorized Users with password resets;

- Inactivate an Authorized HMIS User account if there is a suspected breach or misuse of the HMIS system until a formal investigation has been completed and an outcome reached;

- Delete an Authorized User account if an Authorized HMIS User ceases to be employed at the agency;

- Notify all Agency Users of scheduled HMIS software downtime;

- Monitor and maintain agency data for accuracy and completeness;

- Monitor and report the Agency's compliance with all privacy and security requirements;

- Report all potential and actual breaches in HMIS privacy and security to the HMIS Team in a timely fashion;

- Review and process requests by Clients to inspect and/or correct Client information maintained in the HMIS;

- Maintain licenses and Authorized HMIS User accounts in the system; and

- Ensure the all provider profiles are complete, accurate and up-to-date.

2.6. Authorized HMIS User

Purpose: To define the roles and responsibilities of the Authorized User.

Policy: Prior to accessing the HMIS, all Authorized HMIS Users must complete training and execute an HMIS User Agreement.

Responsibilities:

- Read, sign, and comply with the required HMIS User Agreement;

- Protect the privacy and confidentiality of Client information collected and maintained in the HMIS;

- Ensure that Clients are aware of what information is being collected, stored and shared with the Government and/or other funders

- Notify the HMIS Agency Administrator of all potential and actual breaches in privacy and/or security;

- Comply with the HMIS Policies and Standard Operating Procedures;

- Collect and record all required data elements (UDEs, Funder Assessments, case notes);

- Create passwords that meet requirements contained in section 5.5 of this document;

- Never share passwords and/or Usernames with anyone (including other Participating Agency staff, Supervisors, and Executive Directors); and

- Never store or display written information specifically pertaining to Authorized HMIS User access (e.g., Username and password) in any publicly accessible location.

Section 3.0 Participation Standards

3.1. Participating Policy

Purpose: To define the minimum requirements of Agencies using the HMIS.

Policy: Agencies using the HMIS agree to comply with the HMIS Policies and Standard Operating Procedures.

Procedures: Agencies accessing the HMIS will execute and comply with the HMIS Participating Agency Agreement and as such be considered a Participating Agency.

Participating Agencies are required to:

- Troubleshoot and resolve any Agency-based technical issues;

- Meet the minimum information security, hardware, and connectivity requirements indicated in sections 3.2 and 5.10 of this document; and

- Clean, update, document, and export any data that is to be exported from an agency database. This data must be exported in a format compatible with the import requirements of the HMIS software. The HMIS Team and the HMIS Vendor will provide support and guidance during the migration process.

3.2. HMIS Technical Requirements

Purpose: To define the hardware, security and Internet connectivity requirements for all Participating Agencies.

Policy: Participating Agencies will obtain hardware, security, and Internet connectivity that meets or exceeds the HMIS Vendor recommendations.

Procedures: The Participating Agency will support the hardware, security, and Internet connectivity required to meet the minimum HMIS Vendor's specifications.

Minimum Requirements:

- **Hardware:**

    o Computer running a duo-core processor and at least 2GB of RAM

    o Windows Vista or Windows 7

- **Security:**

  - Virus Protection software: Virus definitions must automatically update;

  - Anti-malware software: Malware definitions must automatically update; and

  - Firewall: Hardware or Software (if software solution, it must automatically update.
  -

- **Internet Browser:**

  - Google Chrome (recommended)

  - Firefox

  - Safari

  - Internet Explorer 11

- **Recommended:**

  - Computer running Microsoft Windows 7 with 4GB of RAM

  - Google Chrome browser that updates as patches become available

Agencies are advised to complete regular maintenance on all workstations or other devices that connect to the HMIS system. This includes, but is not limited to, regularly scheduled virus scans, periodic deletion of temporary/downloaded files and any other maintenance that the agency deems necessary in order to ensure a secure and properly functioning workstation or device. Use of technology that is not compliant to the above noted standards and requirements can result in slow performance and pose a security risk.

3.3. User Licenses

Purpose: To define the allocation of User licenses.

Policy: User licenses will be assigned and managed by the HMIS Team and the HMIS Agency Administrator in compliance with contractual agreements with the HMIS Vendor and HMIS Participating Agency Agreements.

Procedures: The HMIS Team will work with the Participating Agency to determine the number of licenses needed to successfully use the HMIS. A User license is assigned to an Authorized User once the User has successfully completed the Authorized User training. Sharing a license is strictly prohibited.

If a Participating Agency needs additional User licenses, the HMIS Agency Administrator will submit a written request to the HMIS Team indicating the number of required licenses.

The cost of any additional licenses requested may be charged to the Agency. The cost of these licenses are set out in the table in Appendix "D". It is important to note that the fees are on a schedule and as such change from year to year. The table in Appendix "D" will be updated annually to reflect any such changes in license cost.

Section 4.0 Collection, Use and Disclosure of Personal Information

4.1. Compliance with Privacy Legislation

Purpose: To ensure that each Participating Agency is aware of, and complies with the specific conditions imposed by the *Freedom of Information and Protection of Privacy Act* (FOIP), the *Personal Information Protection Act* (PIPA), *Health Information Act* (HIA) or other legislation as applicable, under which the collection, use and disclosure of Personal Information are authorized.

Policy: Participating Agencies must identify the privacy legislation that applies to them so that they understand how this affects their collection, use and disclosure of Personal Information and its storage and management in HMIS. For those Participating Agencies funded by CHF, the FOIP Act applies as a minimum standard. For all other Participating Agencies, the HMIS Participation Agreement requires compliance with PIPA as a minimum standard. Although PIPA may apply to an Agency, HMIS is always subject to FOIP.

Procedures: All Participating Agencies accessing and utilizing Personal Information from the HMIS will confirm with the HMIS Team all contracts and applicable legislation that governs the Personal Information that they collect, use and disclose. This will inform CHF and the Participating Agency about Personal Information that may be entered into HMIS.

FOIP Compliance: HMIS shall be FOIP compliant, even if such compliance is not required by some Agencies using HMIS.

4.2. Obligation to Protect Personal Information

Purpose: To define the custody and control of Client records stored in HMIS.

Policy: A Participating Agency's Personal Information privacy obligations are determined by its custody and/or control of the Personal Information it collects, uses and discloses. "Control" refers to the authority of an Agency to manage a record, including restricting, regulating and administering its use, disclosure or disposition. "Custody" refers to physical possession. HS has control of the Personal Information entered into the HMIS by CHF-funded Agencies whereas CHF has custody of all Client records as prescribed by its Grant Funding Agreement with HS. For all other Agencies, their control of Client records may be limited by funding agreements with other parties whereas CHF has custody of all Participating Agency Client records as prescribed by the Participating Agency Agreement signed with each Agency.

Procedures: The Client is the owner of any information he/she provides to an Agency. Any Participating Agency that collects and stores Client information in the HMIS has control of the data (subject to Funder Agreements that prescribe Personal Information collection, use and disclosure requirements) it enters into the HMIS and has a right to obtain access to that information directly through the HMIS.

The CHF owns the HMIS and under its Participating Agency Agreements, has custody of the data. As the steward of the data, CHF is responsible for the operation and maintenance of the HMIS and has a right to access the data entered into the HMIS.

4.3. Collection of Personal Information

Purpose: To ensure that Authorized Users will only ask Clients for information necessary as authorized by law, to provide services, comply with contractual agreements, support evaluation and research, and improve or better coordinate services.

Policy: Unless the HMIS Participating Agency Agreement otherwise specifies or the CHF otherwise directs in writing, a Participating Agency may only collect or use Personal Information that is necessary for the performance of its obligations, or the exercise of the Participating Agency's rights, under the HMIS Participating Agency Agreement.

Procedures: The following rules apply to the collection of Personal Information:

1. Legislative authority to collect each data element must be verified by the HMIS Team;

2. Client consent cannot be used to override collection that is not legally authorized;

3. The amount of Personal Information collected must be the minimum amount necessary to provide services and to carry out the described Agreement purposes in a reasonable manner; and

4. Personal Information must not be collected "just in case" it might be needed in the future.

A request for additional data fields by an Agency requires prior approval of the HMIS Team. The HMIS Agency Administrator will submit a request in writing to the HMIS Team. The HMIS Team will review the HMIS to ensure that the proposed data element does not already exist and to validate that its collection is authorized by the applicable privacy legislation. If the element does not exist, the HMIS Team will work with the HMIS Agency Administrator to create the data element in the HMIS.

4.4. Manner of Collection of Personal Information

Purpose: To establish direct collection as the primary method for obtaining Personal Information and to allow the Client to know the purpose of the collection of Personal Information and how the information will be used.

Policy: Any data entered into HMIS requires that the FOIP verbal notification be read by the case manager and understood by the Client at the time of collection.

Procedures: The following rules apply to how Client Personal Information is collected:

1. Authorized Users will verbally inform Clients that they are collecting and managing the Client's information in the HMIS (If Participating Agencies prefer, Authorized Users can still collect the Client's written consent in the form of the FOIP Client Consent Form);

2. Authorized Users must read and understand the agency data collection policy around verbal notification;

3. Authorized Users will maintain a copy of the signed Client Consent Form if they chose to use written consent for HMIS data collection; and

4. Authorized Users will not knowingly enter false and/or misleading information into the HMIS.

4.5. Client Awareness of Privacy Rights

Purpose: To promote Client awareness of their privacy rights.

Policy: All Authorized Users must comply with the HMIS Privacy Policy and make the HMIS Privacy Policy available to Clients.

Procedures: Each Participating Agency will post an HMIS Information Poster, as set out in "Appendix E", in intake areas or in a comparable location to provide all Clients an opportunity to learn about the HMIS Privacy Policy. This poster may be graphically formatted to match the Participating Agency's identity.

The HMIS Privacy Policy can be made available in languages and reading levels commonly understood by Clients.

The HMIS Privacy Policy outlines the Client's rights and HMIS practices around privacy and confidentiality, as well as the risks and benefits of providing information for the HMIS.

Participating Agencies must identify someone who can answer a Client's questions about data collection. The person cited should be familiar with the program, and be able to explain why the Personal Information is being collected and how it will be used by and disclosed to other Agencies.

4.6. Use of Personal Information

Purpose: To limit the use of Personal Information collected from Clients only for the purpose for which it was obtained or a consistent purpose; for another purpose with Client consent; or, for purposes allowed under the disclosure sections of the applicable privacy legislation.

Policy: Unless the CHF otherwise directs in writing, the Participating Agency may only use Personal Information if that use is for the performance of its obligations or the exercise of its rights under their Participating Agency Agreement.

4.7. Inter-Agency Personal Information Sharing Through Referral

Purpose: To define Personal Information sharing through referrals between Agencies utilizing the HMIS.

Policy: Data sharing is permitted between Agencies in accordance with the applicable privacy legislation, the FOIP ROI consent of individual Clients and the proper agreement of participating HMIS Agencies.

Procedures: When an Agency refers a Client to a second Agency, the referring Agency may only disclose Personal Information if the Client has signed a FOIP ROI Consent Form. The referring Agency will store a copy of the signed FOIP ROI Consent Form in the Client's physical file for auditing purposes and scan the FOIP ROI Consent Form and attach it to the Client's HMIS record.

4.8. Disclosure of Personal Information

Purpose: To provide parameters for disclosure of Client information by CHF funded Agencies.

Policy: No Personal Information about an identifiable individual shall be disclosed to any individual or organization without the express written consent of the individual, or of a duly authorized representative of the individual, except that Personal Information stored on HMIS may be accessed by duly authorized HMIS Users from the Participating Agency that contributed the Personal Information.

Procedures:

System-wide, Multi-Agency, and Programs not funded by the CHF:

- Aggregate reports released by the CHF will make every attempt not to allow for the disaggregation of included data to prevent the identification of non-funded individual agencies without their consent.

- External requests for data of programs not funded by the CHF will be directed to the Agency Representative of the program. The HMIS Team will only release program information about non-funded programs with permission of the Agency overseeing those non-funded programs.

- The CHF will adhere to all applicable privacy legislation when releasing aggregate reports, making every reasonable effort to protect against the re-identification of records and ensuring that data sets are sufficiently robust to avoid identification of unique individuals.

- The CHF, as custodians of the data held within HMIS, shall be afforded the right to use that data for aggregate reports on an as needed basis as required so long as the data does not directly identify any one agency.

- Data released for research purposes is limited to aggregate, non-identifying information from the predetermined data tables. Data requests for research or statistical purposes that fall outside the data table will be sent to HS through the HMIS Team for Ministerial approval.

Non- Individual Agency:

- Agencies will use and disclose information in accordance with funder contractual obligations, the inter-Agency Data Sharing Agreement and the FOIP ROI Form.

- Agencies will adhere to all applicable privacy legislation and funder contractual obligations when releasing aggregate reports, making every reasonable effort to protect against the re-identification of records and ensuring that data sets are sufficiently robust to avoid identification of unique individuals.

CHF-Funded Programs:

- The CHF reserves the right to produce aggregate reports on all programs that the CHF funds as outlined in the CHF Project Funding Agreement with Agencies receiving those funds.

- The CHF is contractually obligated to provide data to its funders, including HS and HPS, on programs funded by the CHF for the purposes of monitoring and evaluation.

- The CHF System Planners will not request Client information from the HMIS Team. The CHF System Planners will notify funded programs of requests for aggregate data for the purposes of program evaluation. It is incumbent on the Agency to provide such data pursuant to the funding agreement to their assigned System Planner. The Agency can provide the data requested, or if the Agency needs assistance they may request the assistance of the HMIS Team. CHF's System Planners have no authority to directly access Agency data from the HMIS. However, analytic tables for the purposes of trend analysis, funding applications, or community assessment may be generated and provided to System Planners for their expert opinion on such data. These data do not constitute nor satisfy the reporting requirements of CHF-funded agencies to provide data to the CHF for the purposes of program evaluation

- Any additions to the funding portfolio of the CHF may require amendment to the HMIS Participating Agency Agreement.

4.9 Client Right to Request a Correction of Personal Information

Purpose: To ensure that a Client who believes that the information held about them in the HMIS is inaccurate (in error or something omitted), has the right to ask for the information to be corrected.

Policy: Clients have the right to view and receive copies of their records at their request and the right to ask for information to be corrected. Agencies must consider a Client's verbal or written request to receive copies of her/his Client information in the HMIS and/or to correct inaccurate and/or incomplete Client information in the HMIS.

Procedures: Client can make either a verbal or written request to receive a copy of his/her information in the HMIS. Agency Staff will direct requests to view, receive a copy, and/or correct Client information maintained in the HMIS to the HMIS Agency Contact.

When the Agency provides the information to the Client, the Agency must offer to explain any information the Client may not understand.

When making a request to change information in the HMIS a Client must provide documented proof of the change in their information whenever possible.

If the Agency agrees the information is inaccurate or incomplete, the Agency must delete or change the inaccurate and/or incomplete information. If the Agency believes there is a discrepancy between the Agency's observation-based information and the Client's requested changes, the Agency must input what the Client requests, and include a written annotation to the Client's information in the HMIS, indicating the Agency disagrees with the information and the requested change.

When an Agency decides to correct an error, all records containing the Personal Information must be corrected. This includes records in all information systems – paper and electronic. Similarly, when an Agency decides to add omitted information, all systems must be updated. The record should be annotated with the date of the correction. If the change is significant, then the Agency must inform other Agencies to whom the information was previously disclosed.

A Client's request to view and/or correct her/his information can be denied if the Agency believes that reviewing the information may result in harm to the individual or to others. However, this denial must be done with guidance from the Agency Administrator and in accordance with FOIP.

4.10. Client Grievances

Purpose: To ensure that there is a process for handling Client grievances about the use disclosure or management of the Client's Personal Information in the HMIS.

Policy: The Agencies will accept and consider Client questions and/or complaints about the HMIS. If the Participating Agency is unable to resolve the Client's concerns, the Agency will submit the Client's grievance to the CHF.

Procedure: The Agency will respond to all questions or complaints about how the Agency has managed, used, or disclosed the Client's Personal Information in the HMIS. If the Client's concerns are not resolved or if the concerns are related to a potential breach, the Client's grievance must be documented and sent to the CHF. To document the Client's grievance, the Participating Agency Staff will complete and submit the Client Grievance Form to the HMIS Team at the CHF office, located at 308-925 7 Avenue Southwest, Calgary, AB T2P 1A5, Canada. The Agency will not deny services to a Client or the Client's household members for submitting a grievance.

The Agency will also inform the Client of their right to submit a grievance directly to the CHF and provide the Client with the HMIS Team's contact information. The Client can submit their grievance verbally or in writing using the Client Grievance Form, as set out in Appendix "G".

4.11. Reporting a Privacy/Security Breach

Purpose: To ensure that all privacy or security breaches follow the same reporting procedures.

Policy: If an Agency employee becomes aware of a breach or it happens to the employee themselves, it must be immediately reported to the HMIS Agency Administrator and the HMIS Team who will then follow the FOIP procedure.

Procedure:
Different incidents can result in various levels of harm or risk. The HMIS, in consultation with the HS FOIP Coordinator, will investigate the incident to determine the level of harm and any follow-up required to prevent the incident or breach from reoccurring. Typical questions that may be asked during an investigation could include, but are not limited to:

- What were the circumstances that led to the breach?

- Who was involved?

- What information was lost, accessed, altered, or destroyed (includes short term losses)?

- What risk is there as a result of the loss – e.g. was the information encrypted, etc.?

- What level of sensitivity can be attributed to the unauthorized access/loss?

- Is there a need to alert Clients whose information may have been accessed?

- Were all Policies and Standard Operating Procedures in place and being followed?

- Do the policies/practices need to be reviewed and enhanced?

- Could the incident have been avoided?

- Is there a risk of a repeat incident?

- What measures need to be put in place to avoid further similar incidents?

4.12. Records Retention and Disposition

Purpose: To provide records retention and disposal requirements for Client records in the HMIS.

Policy: Client records contained in the HMIS are retained for seven (7) years from the last Client contact. When data has met the retention period it will be archived as aggregate, de-identified information, or subject to HS prior written approval, destroyed. Ministerial approval for destruction will be sought, in addition to outstanding FOIP applications, and outstanding legal issues.

System logs of User access and records of Client data releases and disclosures will be retained for ten (10) years, subject to HS prior written approval.

Procedure: At the end of each calendar year, the HMIS Team will run an audit report of all Client records to determine the last date of Client contact. Client records that exceed the retention period will be reviewed with the Agencies that served the Client to ensure the accuracy of the audit report. Once confirmed, the records will be exported to an aggregate, de-identified archive. Client data, subject to HS prior written approval, will be deleted from the HMIS server(s).

System logs of User access and activities will be maintained for ten (10) years at the office of the HMIS Team. After ten years, and subject to HS prior written approval, the electronic Client records will be destroyed so they cannot be reasonably recovered.

The Client's signed FOIP ROI Consent Form documenting the Client's written consent to release information and disclosure records will be retained for ten (10) years by the Agencies that requested and/or disclosed Client data. After ten years, and subject to HS prior written approval, the Agency will destroy all paper and electronic copies of the information so they cannot be reasonably recovered.

4.13. Data Collection and Entry

Purpose: To define the protocols for data collection and entry into the HMIS.

Policy: Data collected and entered into the HMIS will be accurate and meet the minimum agreed upon data elements.

Procedures: Data elements comprised of both questions and response values fall into three categories: UDEs, PTAs, and FAs. The Client's responses will be entered and stored in the HMIS upon FOIP verbal notification of collection. The Client may refuse to have their information entered into the HMIS.

1. All Authorized Users on the HMIS will ask, collect, and enter the Universal Data Elements into the HMIS.

2. All Authorized Users on the HMIS will ask, collect, and enter their Program Type Assessments into the HMIS.

3. Agencies that fall under FOIP must have the authority to collect Funder Assessments from respective funders to comply with legislation.

Participating Agencies have the responsibility of implementing and managing a procedure for timely entry of Client data. The Agency agrees to ensure all Authorized Users are trained on these procedures.
The Agency is encouraged to reinforce with staff the importance of entering accurate, timely data into the HMIS through staff evaluation and data monitoring.

4.14. Data Quality

Purpose: To set goals and provide information on the process for ensuring quality of the data within the HMIS.

Policy: All Agencies are responsible for the quality of data entered into the HMIS and will participate in a process of improving data quality.

Procedures: All Agencies will strive to collect, enter, and maintain quality data in the HMIS that is timely, complete, accurate, and consistent.

Standards of Data Entry:

- **Timely:** The data entered into the HMIS should include the most current Client information. The Agency will enter intake data into the system within seven (7) working days of the intake.

- **Complete:** The data entered into the system will be as complete as possible and at a minimum, will include all UDEs. Missing and incomplete data can negatively impact the HMIS by under reporting an Agency's and/or the community's efforts. Incomplete Client identifiers can increase the number of duplicate records in the system and also negatively impact the usefulness of the HMIS.

- **Accurate:** The data entered into the HMIS will reflect accurate Client identifiers and the current status of Clients. If information is unknown to the Client or the Client does not answer the question, the Agency will identify it as such as opposed to selecting an inaccurate response. Due to the critical nature of data accuracy, the Agency will place accuracy as a priority and encourage it at all levels. The Agency will routinely monitor for errors, including those resulting from misspellings, transposing numbers, inter-changing name fields, and illegible intake forms. Inaccurate Client identifiers and status can lead to duplicate Client files and misleading and wrong information. **Inaccurate data results in a misrepresentation of the nature of homelessness in Calgary and thus obstructs efforts to prevent and end homelessness.**

- **Consistent:** The data entered into the system should be collected and entered into the system in the same way by all Users. All Users will be educated on the meaning of the questions being asked and the appropriate response categories.

- **Exceptions:** if it is impossible to contact the Client when an assessment is due, the Agency may answer only those questions they can with absolute certainty.

Section 5.0 Operation and Technical Standards

5.1. Training

Purpose: To delineate HMIS training requirements and benefits.

Policy: Training is required for all HMIS Users prior to accessing the HMIS and is provided by the HMIS Team on a regular basis.

Procedures: The HMIS Team will provide regular training to Participating Agency staff on the use of HMIS. Upon completion of training, Agency staff should reasonably understand how to enter and extract data from the HMIS. Participating Agency staff will be permitted access to the HMIS once they have completed the Basic User Training, reviewed the Policies and Standard Operating Procedures, and submitting a signed copy of the HMIS User Agreement to the HMIS Team.

Basic User Training Objectives:

- Introduction to HMIS;

- Review system privacy and security protocols;

- Understand data quality requirements;

- Discuss support request procedures;

- Learn how to log on to system;

- Learn how to record Client consent to release information; and

- Learn how to enter agreed upon Client and program data

5.2. User Access, Awareness and Sanctions

Purpose: To secure access to the HMIS.

Policy: Only Authorized Users will have access to the HMIS. Each HMIS User will have an individual Username and password that may not be shared with anyone for any purpose. If an Authorized User no longer requires access to the HMIS, the HMIS Agency Administrator will notify the HMIS Program Manager and their access will be terminated.

Procedures: The Authorized User will be issued a unique username and temporary password after the Authorized User completes User Training, verifies they have read the Policies and Standard Operating Procedures, and submits a signed HMIS User Agreement.

If an Authorized User has lost or forgotten his/her password, he/she can request a password reset from the HMIS Agency Administrator or the HMIS Team.

If an Authorized User no longer requires access to the HMIS the Authorized User's credentials will be removed from the HMIS.

The Agency is responsible for all Authorized User activity on the HMIS and must ensure only appropriate staff have access.

If there is a suspected breach and/or misuse of the system, an Authorized User's access may be suspended until such time as the issue is resolved.

Access Monitoring Plan

The Calgary HMIS software application maintains an audit trail that tracks User log-in attempts for a minimum of six months. The Calgary HMIS software application maintains an audit trail that tracks the deletions to Client records (including the actual assessment entry, date deleted, and Username) for a minimum of six months and a record of deleted Client records (case number, intake information, data deleted, and Username) for a minimum of one year.

The Calgary HMIS software application records transactional data on all other Client information for historical and audit purposes. Each entry reflects the User that created the entry and the date and name of the User that made the most recent modification. Bowman Systems' ServicePoint™ software is designed to automatically fulfill these obligations.

The HMIS Agency Administrator has the ability to review these logs for its Agency's Users to determine unauthorized or inappropriate access to Calgary HMIS Client records.

Agencies should also institute internal monitoring methods to ensure compliance with the HMIS Policies and Standard Operating Procedures.

Agencies may be required to demonstrate that they are complying, and/or may be subject to technical and/or policy monitoring.

All Users and custodians are obligated to report suspected instances of noncompliance and/or security violations to an HMIS Agency Administrator, who will inform the HMIS Team, who will then follow FOIP procedures dependent on the privacy or security concern.

Violations and Sanctions:

All reported potential violations of any security protocols will be investigated by the CHF with the advice of the HMIS Advisory Group.

Any User found to be in violation of security protocols will be sanctioned accordingly.

Sanctions can include, but are not limited to:

- A formal letter of reprimand;

- Suspension of system privileges;

- Revocation of system privileges;

- Termination of employment for Participating Agency staff;

- Criminal prosecution; and/or

- Civil prosecution.

A Participating Agency's access may also be suspended or revoked if serious or repeated violations of the standard operating procedures occurs by Participating Agency Users.

All Calgary HMIS sanctions will be imposed by a team comprised of the Calgary HMIS Team and the VP of Strategy.

All CHF funded program breaches will be reported by the CHF to the HS by the HMIS Team.
Calgary HMIS Sanctions can be appealed to the HMIS Advisory Group.

Police reporting and/or criminal prosecution sanctions will be recommended by the HMIS Team.

5.3. User Account Procedures

Policy: The Calgary HMIS Team may create a new User ID, inactivate a current User ID or delete a current User ID for eligible individuals based on the following procedure. The activation/inactivation/deletion procedure is tracked via the ServicePoint™ software.

Purpose: To inform all parties involved with the Calgary HMIS of the requirements to activate/inactivate/delete a Calgary HMIS User.

Procedures: If the Participating Agency wants to authorize system use for a new User, the authorized designee must:

- Determine the access level of the proposed Calgary HMIS User according to those outlined in Calgary HMIS Policies and Standard Operating Procedures: User Access levels; and

- Authorize the creation of a User account for the specified individual once the individual has completed HMIS training and complete and submit, to the HMIS Team, a signed HMIS User Agreement that designates the access level.

The proposed Authorized HMIS User must:

- Attend applicable training (once enrolled by the Agency Administrator) as described in the HMIS Policies and Standard Operating Procedures; and

- Execute an Authorized HMIS User Agreement.

The Agency Administrator must:

- Enroll the potential Calgary HMIS User in the required training; and

- Sign and submit the HMIS User Agreement for new staff.

The Calgary HMIS Team shall:

- Review HMIS records about a potential Authorized HMIS User to ensure that the individual does not have previous policy and procedure violations that would prohibit access to the Calgary HMIS, (as determined by the HMIS Team);

- Verify that the required documentation (HMIS User Agreement) has been correctly executed and submitted; and

- Verify that required training has been successfully completed.

If the Participating Agency wants to inactivate or delete a current User, the Agency Admin (or an authorized designee) must:

- Inactivate or delete the HMIS account of a specified User and notify the HMIS Team by email.

5.4. User Types and Data Access

Purpose: To determine the appropriate type of access for each User.

Policy: User licenses will be assigned at a security level, as set out in Appendix "F", that allows no more information than needed to perform job responsibilities.

Procedures: The HMIS Agency Administrator, in conjunction with the HMIS Team, will determine the physical access controls appropriate for the Agency's organizational settings and the Agency's Users.

5.5. User ID and Password Specifications

Purpose: To delineate HMIS User ID protocols and Password specifications.

Policy: The HMIS system, all electronic HMIS data, and any device used to access the HMIS system must have, at a minimum, a User authentication system consisting of a Username and a password.

Procedures: User Access levels will be approved by the Agency's HMIS Agency Administrator in consultation with the HMIS Team. The access levels assigned to the User should be reflective of the access a User has to Client-level paper records and should be need-based. The HMIS Team will issue the User ID and password to the User. User ID and Passwords are to be assigned to individuals who have passed the Calgary HMIS Training and who have understood and signed the HMIS User Agreement.

The HMIS Team will provide the Authorized User (or their HMIS Agency Administrator) with a temporary password after the submission of the signed HMIS User Agreements. After logging in to the system for the first time with the temporary password, the User will create a personal password that is only known to them.

If an Authorized User unsuccessfully attempts to log onto the system three times, the User ID will be "locked out," access permission will be revoked, and the Authorized User will be unable to gain access until their password is reset. To reset a password, the Authorized User must contact their HMIS Agency Administrator or the HMIS Team.

User ID and Password Specifications:

- The User ID will be the first initial and full last name of the User. If a User has a first initial and last name that is identical to a User already in the system, the User ID will be the first initial and last name plus the numbers "01";

- Passwords will reset every forty five (45) days;

- You may not use a password you have used recently;

- Password must be at least eight (8) characters long;

- Passwords must include at least four (4) numbers and four (4) characters;

- Passwords may not use, or include, the Username, the HMIS name, or the HMIS Vendor's name; and

- A one-time password will be provided by the HMIS Team for initial entry into the HMIS application; upon entry the Authorized User will create a password that is only known to them.

5.6. Technical Support

Purpose: To provide reasonable expectations for HMIS technical support by the HMIS Team.

Policy: Technical support after the End Users initial training in the access and use of the HMIS System is available to all HMIS Users and is provided by the HMIS Team on a regular basis.

Procedures: The HMIS Team will provide regular helpdesk support hours during business hours and after hours if an emergency arises. Helpdesk hours are available from 8:30AM to 4:00PM Monday through Friday, as set out in the Participating Agency Agreement. The helpdesk can be reached by calling (403) 718-8545 or emailing the HMIS Team at HMIS@calgaryhomeless.com. Depending on the nature, current volume of requests, and urgency of the need, the support may need to be scheduled. The HMIS Team will call or email the User within 24 hours of the request to either provide a solution or to schedule a response.

The HMIS Team will assist in isolating problems related to the Agency's hardware (i.e. servers, routers, workstations, and firewalls), internet connectivity, or software installed on the Agency's hardware. Once identified, the Agency will need to seek assistance through third-party technical support, internal technical support, manufacturers, or service providers to resolve these problems.

Type of Support Request that can be Made Directly to the HMIS Team:

- Accessing the system;

- Troubleshooting software issues;

- Any suspected security problems;

- Any suspected security or privacy breaches;

- Data quality support;

- Training and refreshers;

- Development of ReportWriter data downloads;

- Setting up a User Account;

- Purchasing User licenses;

- Additions or alterations to Assessments;

- Additions or alterations to Picklists and Dropdown Menus; and

- Development of ART Reports.

5.7. Legacy Data Migration Options and Procedures

Purpose: To inform Agencies of the options and process for migrating an Agency's legacy data into the HMIS.

Policy: Agencies can import identifiable Client data if it meets specific data privacy and import standards.

Procedures: The HMIS Team will establish data quality and completeness thresholds to be met before data transfers are approved. All Agencies migrating data from an Agency database must first clean, update, document, and export data in a format compatible with the import requirements of the HMIS software. The HMIS Team and the HMIS Vendor will provide support and guidance during the migration process. The CHF will not subsidize the cost of migrating data that are only relevant to a single Agency or that requires extensive analysis from both the HMIS Team and the HMIS Vendor.

The Agency will need to provide the following to the HMIS Team and the HMIS Vendor:

- Data Dictionary – complete with table and field descriptions, data types, data formats, ranges of values, acceptable values, foreign keys, etc.

- Data Relationship Diagram – detailed mapping of all relative data

- Sample Data – a sample of 10-20 Client records that includes the full set of all data tables and fields for those records.

5.8. Data Integration Options and Procedures

Purpose: To inform Agencies of the options and process for integrating their data into the HMIS.

Policy: Agencies can integrate identifiable Client data if it meets specific data privacy and import/export standards.

Procedures: The HMIS Team will establish data quality and completeness thresholds to be met before data transfers are approved. All Agencies integrating data through regular data transfer schedules from an Agency database must first clean, update, document, and export data in a format compatible with the import requirements of the HMIS software. The HMIS Team and the HMIS Vendor will provide support and guidance during the initial migration and ongoing integration process. The CHF will not subsidize the cost of integrating data that are only relevant to a single Agency or that requires extensive analysis from both the HMIS Team and the HMIS Vendor.

The Agency will need to provide the following to the HMIS Team and the HMIS Vendor:

- Data Dictionary – complete with table and field descriptions, data types, data formats, ranges of values, acceptable values, foreign keys, etc.

- Data Relationship Diagram – detailed mapping of all relative data

- Sample Data – a sample of 10-20 Client records that includes the full set of all data tables and fields for those records.

5.9. HMIS Software Updates and Upgrades

Purpose: To provide information to HMIS Users on the process of updating and upgrading HMIS software.

Policy: The HMIS will be updated and/or upgraded to ensure the system is running in its most secure and stable version.

Procedures

- The HMIS Team will notify the Agency of all updates and/or upgrades to the HMIS through E-mail to the HMIS Agency Administrator, and on the HMIS ServicePoint™ Dashboard.

- The notice will include the impact of the update and/or upgrade on the system, data, and reports;

- All updates and/or upgrades will occur no sooner than one week after the notice; and

- HMIS Agency Administrator must read the impact notification and notify the HMIS Team of all concerns regarding the impact of the update and/or upgrade within 48 hours of the scheduled update and/or upgrade.

5.10. Agency Security Specifications

Purpose: To ensure data accessed at the Agency level is protected and meets baseline security standards.

Policy: The Agency must comply and monitor HMIS security at their Agency.

Procedures: The CHF protects the information on the HMIS server and access to the server. The Agency is required to implement the security standards set forth in this policy to protect the Client data being entered into the HMIS. The security at the Agency includes, but is not limited to, password protection, virus protection, malware protection, firewall protection, workstation security and media disposal. The CHF recommends Agencies refrain from downloading sensitive Client information to Agency workstations and servers.

- **Password Protection:** The Agency will ensure all Users understand that an HMIS Username and password cannot be shared with anyone and is not transferable. All HMIS activities carried out under a User account are maintained in a log and the User assigned to that account will be responsible for activities that occur under that User's account;

- **Virus Protection:** The Agency will purchase, install, and maintain commercially available virus protection software on all computers and servers accessing the HMIS. Virus protection must automatically scan files as they are accessed by Users on the system where the HMIS data is accessed and/or stored. The virus protection software must automatically and regularly update virus definitions;

- **Malware Software:** The Agency will purchase, install, and maintain commercially available malware protection software on all computers and servers accessing the HMIS. Malware protection must automatically scan the system where HMIS data is accessed and/or stored. The malware protection software must automatically and regularly update the malware definitions;

- **Firewall Protection:** The Agency must protect the HMIS from malicious intrusion by using a secure firewall. Each individual workstation does not need a firewall, as long as there is a firewall between that workstation and any systems, including the Internet and other computer networks, located outside of the organization;

- **Workstation Security:** The Agency must staff computers at all times if such computers are used to collect and/or store HMIS data and are stationed in public areas. When any computer used to collect and/or store HMIS data is not in use and staff is not present, steps should be taken to ensure the computers and data are secure and not usable by unauthorized individuals. When any workstation used to collect and/or store HMIS data is not in use for a short-period of time, a password protected screen saver should automatically turn on. Password protected screen savers are a standard feature with most operating systems and the amount of time can be regulated by an Agency;

- **Data Transfer Security:** Client personal information is not removed from the agency's premises without authorization. This includes carrying information on a cell phone or USB drive. Client personal information transmitted by email is encrypted or password protected. Transitory or obsolete electronic and paper records are regularly destroyed using appropriate methods.

- **Media Disposal:** The Agency will ensure only Authorized Users access electronic and print media containing Client information. Agencies must use proper methods to destroy HMIS data on electronic and print media (e.g. shredding print media and erasing the magnetic field of electronic media (i.e. hardware, floppy disks, magnetic tapes) to ensure data cannot be reconstructed, recovered, or restored.

5.11. Central Server Operations and Location

Purpose: To ensure the data on the server is secure and resides within Canada.

Policy: The CHF requires the HMIS vendor to uphold all federal, provincial and local security standards and will receive regular security status reports from the vendor.

Procedures:

- **Availability:** The CHF provides oversight management of the HMIS and the HMIS Vendor's services. The HMIS Vendor is contractually obligated to ensure that the HMIS is available to Authorized Users on a consistent and continual basis except, but not limited to, the following: natural disasters, widespread power outages, and scheduled downtime. If the Vendor does not meet this obligation, the Vendor is required to make a penalty payment to the CHF. In the event of an unscheduled downtime; the HMIS Team will email the HMIS Vendor to re-establish access to the system and notify HMIS Agency Administrators when the system went offline and when access is re-established. For upgrades, updates, and scheduled downtimes, the HMIS Team will notify HMIS Agency Contacts one week prior, providing the purpose, the anticipated impact, and projected time for re-establishing access. The HMIS Team will keep a log of all scheduled or unscheduled downtimes indicating causes and corrective actions.

- **Storage Location:** The servers that house all HMIS data are located in Cambridge ON, Canada. The specific address is kept confidential for security purposes and is on file at the CHF headquarters.

- **Access:** Central server, mini-computer, mainframe hosting database, and/or application software is kept in a secure room with appropriate environmental controls and physical access to the system is monitored and logged. User authentication for all individuals accessing data on the server is required.

- **Encryption:** All transmission of data between the Agencies terminal and the server are protected with an industry standard, 128-bit encryption by VeriSign;

- **Virus Protection:** Server-side virus protection automatically scans files as they are accessed by Users on the system where the HMIS application is housed. Virus protection is automatically updated. Server-side firewalls protect the HMIS server from malicious intrusion.

- **Backup and Recovery Services:** Server-side disaster protection and recovery creates a back-up of the system and database to a secure location off-site; location of the system and database server is secure and equipped with temperature control and fire suppression systems as well as surge suppressors; Routine data back-up to tape or other format that is stored securely off-site within Canada; and

User Monitoring: The System is able to provide a User access log upon request that indicates the time of access, the duration, and the information that was viewed, altered or deleted

Appendix A: Participating Agency Agreement

PARTICIPATING AGENCY AGREEMENT
(THIS "**AGREEMENT**")

Calgary Homeless Management Information System ("**HMIS**")

This Agreement is effective as of [Month DD, 2015] (the "**Effective Date**") between the Calgary Homeless Foundation ("**CHF**"), and [insert agency name] (the "**Agency**"), regarding HMIS access and use in connection with any individual (the "**Client**") who receives services offered by the Agency from time to time and from whom the Agency may collect "Personal Information" (as defined in the Freedom of Information and Protection of Privacy Act (Alberta) ("**FOIP**")).

Whereas:

A.   HMIS is a web based, electronic client management information system managed by CHF that provides a standardized assessment of client needs, individualized service plans and service records;

B.   The intent of HMIS is to enable greater depth in the understanding of the nature of homelessness, to develop policies and initiatives to address homelessness, coordinate case management services and ultimately end homelessness in Calgary; and

C.   HMIS is predicated on shared access (based on client consent) among community agencies, organizations and groups in the homelessness serving sector in Calgary.

In consideration of the mutual covenants and agreements contained herein, the parties agree as follows:

1.   TERM

This Agreement shall be in effect from the Effective date and shall be renewed automatically on July 1 of each consecutive year until this Agreement is terminated by either party with 30 days written notice to the other party, or if this Agreement is terminated pursuant to Section 8 of this Agreement.

2.   FEES

At the request of CHF, the Agency agrees to pay, in a timely manner, the initial and the annual HMIS user fees (which are subject to increase, as discussed below), such fees as more accurately set out in Appendix "A" attached hereto (the "**Fees**"). The Agency acknowledges that the Fees may be increased from time to time due to the fact that select or a portion of the Fees are controlled and set by a third-party HMIS service-provider. If said HMIS service-provider increases the Fees, CHF shall advise the Agency of such increase at its earliest opportunity, and in any event, no later than June 1. Failure by the Agency to pay the Fees will constitute a breach of this Agreement.

3.   CONDITIONS PRECEDENT

This Agreement shall become effective subject to and conditional upon the satisfaction of the following conditions:

(a)   CHF shall receive each of the following documents in form and substance satisfactory to CHF, acting reasonably:

     (i).   a duly executed copy of this Agreement; and
     (ii).   a duly executed copy of the form of user agreement (the "User Agreement") attached to the Calgary Homeless Management Information System: Policies and Standard Operating Procedures manual, a copy of which has been provided to the Agency herewith (the "**P&P**").

4.   CHF POSITIVE COVENANTS

CHF hereby covenants and agrees with the Agency that CHF shall:

(a)   provide HMIS training to any personnel, contractor, volunteer or other representative of the Agency who has been authorized to access HMIS (each, a "**User**");

(b)   be responsible for ensuring HMIS is implemented so that it is functional and usable by the Agency for the purposes for which it is intended;

(c)   provide basic technical support including general trouble-shooting and assistance with standard report generation, such technical support to be made available from 8:00 a.m. to 4:00 p.m., Monday through Friday, excepting holidays, and at the discretion of CHF, such technical support may be available after the above-mentioned hours;

(d)   make available and provide templates or other documents that would be reasonably required for HMIS use, including informed Client consent forms;

(e)   adhere to all ethical practices, current standards and applicable laws when data mining, data analyzing, or releasing any reports derived from HMIS in whole or part, and making every reasonable effort to protect against the re-identification of any records to avoid identification of unique individuals; and

(f)   upon written request by the Agency, remove or cause to be removed from HMIS any and all Client information stored in such Client's record, including any Personal Information and in the event that HMIS ceases to exist, provide the Agency with written notice of the same, and within a reasonable amount of time thereafter, provide the Agency with an electronic copy of the Agency's data which has been collected and maintained in HMIS up to and including the date of termination or the date of last use of HMIS and shall certify that permanent removal of the Agency's data has occurred.

5.   THE AGENCY`S POSITIVE COVENANTS

The Agency hereby covenants and agrees with CHF that the Agency shall:

(a)   comply, at all times, with the following documents, copies of which have been provided to the Agency herewith:

(i).   the P&P; and
(ii).   the User Agreement;

(b)   only allow Users to access HMIS, and each such User shall, prior to obtaining access to HMIS, complete required training for use of HMIS, and only after completion of such training, may such User be given an system ID and password for use of HMIS;

(c)   make best efforts to ensure, and continue to ensure that: (i) all Users attend periodic training provided by CHF (or a representative on behalf of CHF), (ii) all Users are sufficiently trained to use HMIS, and (iii) obtain, review and disseminate any HMIS information updates provided to the Agency by CHF;

(d)   perform and participate in any audits in relation to HMIS as reasonably required by CHF from time to time or as set out in P&P and which may occur following the termination of this Agreement pursuant to Section 8 of this Agreement;

(e)   notify CHF immediately in writing of any of the following events:

(i).   any security breach, FOIP breach, error or malfunction of HMIS that compromises, or could reasonably compromise, the security of HMIS;

(ii).   if the Agency or any User has breached, or the Agency reasonably believes that the Agency or any User may have breached, this Agreement or the P&P, and the Agency shall make best efforts to remedy such breach immediately; and

(iii).   if the Agency becomes of aware of any misuse of HMIS by a User or a user of any other Participating Agency;

(f)   at all times, take any and all actions, and inform each Client who supplies the Agency with any Personal Information to be used in HMIS, in the following manner:

(i).   with the express consent from the Client, collect from such Client only the Personal Information that the Agency is authorized to collect for the provision of the Agency's services and to retain the Personal Information for a reasonable period of time and such information shall be collected and retained only for the purposes for which the Personal Information was originally collected;

(ii).   post notices or present notices to each Client concerning the Privacy Policy at the time and location of intake, such that each Client has the opportunity to read the notices prior to providing consent;

(iii).   in obtaining consent, take all reasonable steps to ensure that the Client has understood the information provided; and

(iv).   after a reasonable period of time from the date the Agency ceases providing services to a Client, the Agency shall terminate access to such Client's record and all of such Client's Personal Information, including all of its data elements, such that access to such Client's record shall only be available to CHF;

(g)   adhere to all ethical practices, current standards and applicable laws when data mining, data analyzing, releasing any reports derived from HMIS in whole or part, or otherwise using HMIS in any manner, and making every reasonable effort to protect against the re-identification of any records to avoid identification of unique individuals; and

(h)   establish and maintain an internal Agency policy that addresses procedures related to Client confidentiality, electronic records retention, staff misconduct and violations in relation to both Personal Information and any other confidential information as it relates to HMIS use and that is understood and signed by every officer, director, employee, contractor, or volunteer of the Agency, and the Agency shall be responsible for any oversight, error, negligence or other injurious act or omission in relation to any data or information used or disclosed by the Agency or any User.

6.   THE AGENCY`S NEGATIVE COVENANTS

The Agency hereby covenants and agrees with CHF that the Agency shall not:

(a)   intentionally or negligently disclose, or caused to be disclosed, any User's HMIS login IDs or passwords to any individual;

(b)   intentionally cause corruption, lost functionality or insecurity of HMIS in any manner, nor shall the Agency intentionally permit any person to make any unauthorized access or unauthorized modification, addition, deletion or any other change to HMIS, the information contained within HMIS, or intentionally interfere with normal system operations;

(c)   input or solicit any information from a Client for input into HMIS unless the Agency is authorized for service provision or to conduct evaluation or research that is directly related to the type and nature of services provided by the Agency;

(d)   where a Client has previously consented to sharing their Personal Information with other Participating Agencies, and then chooses to revoke such consent, the Agency shall immediately stop sharing the Personal Information upon the Client's completion of a Client Consent Cancellation form attached to the P&P; or

(e)   use HMIS with the intent to defraud any person, or to conduct any illegal activity.

7. INFORMATION SHARED BY THE AGENCY

(a) In entering into this Agreement, the Agency agrees to providing certain information to the CHF in order to both assist the CHF in fulfilling its responsibilities as system planner in Calgary's System of Care and to allow both the CHF and the Agency to participate in evidence based advocacy, the following list of data elements, (the "Shared Data"):

(i) Client basic demographics;
(ii) Universal Data Elements;
(iii) Program Entry and Exit;

(b) Without limiting any other terms or conditions of this Agreement, the parties agree and acknowledge that the CHF may only use the Shared Data, or parts thereof, for the purposes of:

(i) Satisfying internal CHF data analysis requests for internal CHF uses only;
(ii) Sharing external to the CHF, data analysis that is based in part on information obtained from the Shared Data. These reports shall contain summarized or aggregated references to the Shared Data.

(c) Notwithstanding any other terms or conditions of this Agreement, the Recipient shall not use the Shared Data, or parts thereof, to report on any data that relates directly to:

(i) An identifiable individual or data that may be used to identify any individual; or
(ii) The Agency.

8. TERMINATION

(a) Where either party breaches this Agreement, unless, in the reasonable opinion of CHF, such breach is irremediable or creates an adverse impact, damage, injury or any other repercussions to any Client, CHF, or any other Participating Agency or to the HMIS system, the breaching party shall be given not more than 15 days to remedy such breach, subsequent to which, if the breach has not been cured by the breaching party, the non-breaching party shall have the option to extend the time allotted to remedy the breach or to terminate this Agreement immediately.

(b) Notwithstanding Section 8(a), above, CHF, acting reasonably, may terminate this Agreement or suspend access to HMIS at any time, on reasonable grounds, if an allegation or actual incident arises regarding a potential or actual breach of this Agreement, until such allegations or breach, as applicable, are resolved. In the case of suspension, this Agreement shall remain in effect.

(c) Upon termination of this Agreement, or if HMIS use has been suspended for a period of 30 days or more, CHF shall, within a reasonable period of time, provide the Agency with an electronic copy of the Agency's data which has been collected and maintained in HMIS up to and including the date of termination or suspension, as applicable, or on the date of last use of HMIS, and in each case, CHF shall certify that permanent removal of the Agency's data has occurred.

9. INDEMNITY

(a) The Agency shall, both during and following the termination of this Agreement, indemnify and save harmless CHF and any other Participating Agency, its officers, directors, employees, contractors, volunteers or other representatives from and against all claims, losses, damages, costs, expenses and other actions made, sustained, brought, threatened to be brought or prosecuted, in any manner based upon, occasioned by or attributable to any injury or death of a person, breach of this Agreement or loss or damage to property caused or alleged to be caused by any wilful or negligent act, omission or delay on the part of the Agency or its officers, directors, employees, contractors, volunteers or other representatives in connection with anything purported to be or required to be provided by or done by the Agency pursuant to this Agreement or in connection with or suffered as a result of use of HMIS or participation in any activities in whole or part related to HMIS, except that CHF and any Participating Agency shall not claim indemnity under this Section 8 to the extent that the injury, loss or damage has been caused by the gross negligence or willful misconduct of CHF or the negligence or wilful misconduct of any other Participating Agency. For the purposes of this Section 8, a Participating Agency does not include the Agency.

(b) CHF takes no responsibility whatsoever for any data or information derived or exported, in whole or part, from HMIS and used separate or apart from HMIS.

10. **GENERAL**

(a) **Amendment.** This Agreement may only be modified or amended by written agreement executed by both parties.

(b) **Survival.** Notwithstanding the termination of this Agreement, the provisions of Section 4.0 Collection, Use and Disclosure of Personal Information of the P&P and all consequent rights, obligations and liabilities thereunder shall survive the termination of this Agreement.

(c) **Waiver.** The failure of either party to enforce at any time or for any period of time any of the provisions of this Agreement shall not constitute a waiver of such provisions or the right of either party to enforce each and every provision.

(d) **Governing Law.** This Agreement shall be governed by the laws of the Province of Alberta and of Canada applicable therein.

(e) **Force Majeure.** The non-performance by either party of an obligation hereunder shall be excused to the extent that performance is rendered impossible by fire, flood, or other act of God, governmental acts, orders or restrictions.

(f) **Counterpart.** This Agreement may be executed in several counterparts, each of which when so executed shall be deemed to be an original and such counterparts together shall constitute one and the same instrument.

(g) **Notices.** Any and all notices which may be given by one of the parties to the other shall be given by mail (if no mail strike), facsimile or email, or may be hand delivered to the other party at the following address:

in the case of CHF, to:

> Calgary Homeless Foundation
> Attention: Manager, HMIS
> 925 7th Avenue SW, Suite 308
> Calgary, Alberta, T2P 1A5
> Telephone: (403) 718-8537
> Fax: (403) 262-2924
> Email: hmis@calgaryhomeless.com

in the case of the Agency, to:

> [insert name of Agency]
> Attention: •
> [insert address]
> Calgary, Alberta [insert postal code]
> Telephone: (•) •-•
> Fax: •
> Email: •

and such notices shall be deemed to have been received five (5) business days after mailing if forwarded by mail and the following business day if forwarded by facsimile, email or hand-delivery. The aforementioned address of either party may be changed at any time by giving five (5) business days prior notice to the other party in accordance with the foregoing.

(h) **Assignment.** Neither party shall assign this Agreement without the written consent of the other party.

(i)   **Entire Agreement.** This Agreement and appendices attached hereto set forth the entire agreement and understanding between the parties and supersede and cancel all previous negotiations, agreements, commitments and writings in respect of the subject-matter hereof and there are no understandings, representations, conditions made or assumed by the parties, other than those expressly contained in this Agreement. Neither party shall be bound by any term, clause, provision or conditions save as expressly provided herein or as duly set forth on or subsequent to the later of the Effective Date and the date of execution of this Agreement in writing signed by duly authorized officers of the parties.

IN WITNESS WHEREOF, the parties have entered into this agreement as of the Effective Date:

CALGARY HOMELESS FOUNDATION

Per: _____   Date: _____

Diana Krecsy
Name of authorized signing officer
(please print)

President & CEO
Title / Office held
(please print)

[AGENCY NAME]

Per: _____   Date: _____

Name of authorized signing officer
(please print)

Title / Office held
(please print)

Appendix B: Agency Admin Agreement

HMIS Agency Administrator User Agreement
User Policy, Responsibility Statement, and Code of Ethics
CALGARY HOMELESS MANAGEMENT INFORMATION SYSTEM (HMIS)

Date: _____

User (print full name):

_____

Employee Work Number (_____) _____ Ext: _____

Employee E-Mail Address:

_____

Agency Name:

_____

Program Name:

_____

I understand that I will be allowed access to confidential information and/or records in order that I may perform my specific job duties and none other. I further understand and agree that I am not to disclose confidential information, and/or Client records without the prior written consent of the Calgary Homeless Foundation, unless such disclosure is required by law.

User Responsibilities:

HMIS Agency Administrators have separate and distinct responsibilities regarding communication and dissemination of HMIS Policies and Procedures as well as Calgary Homeless Foundation Data Quality standards. Initial each item below to indicate your understanding and acceptance of the proper use of this access. Failure to uphold the responsibilities set forth below is grounds for removal of Agency Admin role from HMIS.

_____   I am responsible for the data entry completed by those HMIS Users in my respective program(s). This includes adhering to the following documents:
- HMIS Policies and Procedures
- HMIS User Agreement
- HMIS Data Quality Plan
- HMIS Data Collection Policy

_____   I understand I am the link of communication between the Calgary Homeless Foundation and the HMIS Users at my program

_____ I will disseminate all pertinent information to HMIS Users and other staff at my program as necessary

_____ I am aware of the timelines and deadlines applied to information input into HIS ServicePoint and will communicate with the appropriate person(s) at Calgary Homeless Foundation should I be aware that these deadlines will not be met

_____ I am responsible for the Admin module in ServicePoint as it pertains to my program(s) and will keep all information in this module up to date

_____ I will notify the CHF HMIS team of any and all HMIS Users which need to be added or removed from my program(s)

_____ I will respond to all requests for data according to the guidelines of the FOIP Act and policies outlined by the Calgary Homeless Foundation on behalf of Human Services

_____ I will notify my HMIS Agency Contact if I notice or suspect a breach in privacy or security.

_____ I have been given the opportunity to read the Calgary Homeless Management Information System: Policies and Standard Operating Procedures, and I will comply with them to the best of my ability.

Ethical Data Usage:

Once you have completed training and signed your HMIS Agency Admin User Agreement, you are entitled to access to the Calgary HMIS at the level of Agency Administrator. In addition to the responsibilities listed above, you must also adhere to the following principles of ethical data usage.

- Authorized Users will only ask Clients for information necessary to providing services, comply with contractual agreements, and to improve or better coordinate services;
- Authorized Users will ensure that Clients understand that their data is being collected and managed in the HMIS using the FOIP Verbal Notification as a guideline;
- Authorized Users will obtain a signed Release of Information (ROI) form before sharing client data with an outside program/agency on the HMIS
- Authorized Users will maintain a copy of the ROI Form;
- Authorized Users will not knowingly enter false and/or misleading information into the HMIS;
- Authorized Users will only use data in accordance with the Privacy Policy; and
- The Calgary Homeless Foundation, Participating Agencies, and Authorized Users will adhere to the HMIS Privacy Policy.

By affixing my signature to this document, I acknowledge that I have been apprised of the Calgary HMIS Policies and Standard Operating Procedures concerning access, use, maintenance, and disclosure of confidential information and/or records that shall be made available to me through my use or the Calgary HMIS.

User Signature   Date

Agency Contact Signature   Date

Appendix C: HMIS User Agreement

User Agreement
User Policy, Responsibility Statement, and Code of Ethics
CALGARY HOMELESS MANAGEMENT INFORMATION SYSTEM (HMIS)

Date training was completed: _____

User (print full name):

_____

Employee Work Number (_____) _____ Ext: _____

Employee E-Mail Address:

_____

Agency Name:

_____

Program Name:

_____

I understand that I will be allowed access to confidential information and/or records in order that I may perform my specific job duties and none other. I further understand and agree that I am not to disclose confidential information, and/or Client records without the prior written consent of the Calgary Homeless Foundation, unless such disclosure is required by law.

User Responsibilities:

Your User ID and Password give you access to your agency's data in the Calgary HMIS. Initial each item below to indicate your understanding and acceptance of the proper use of this access. Failure to uphold the confidentiality standards set forth below is grounds for suspension of HMIS User privileges until such time as the issue is resolved.

_____   My User ID and Password are for my use only and must not be shared with anyone.
_____   I must take all responsible means to keep my User ID and Password physically secure.
_____   I understand that the only persons who may view Client files in the HMIS are authorized Users and the Client to whom the information pertains.
_____   I may only view, obtain, disclose, or use the database information that is necessary to perform my job and none other.
_____   I will not leave a workstation where I am logged into HMIS unattended.
_____   I will log off of HMIS before leaving the workstation, even for a short time.
_____   I will assure that any printouts/hard copies of HMIS information will be properly secured.

_____   I will notify my HMIS Agency Contact if I notice or suspect a breach in privacy or security.

_____   I have been given the opportunity to read the Calgary Homeless Management Information System: Policies and Standard Operating Procedures, and I will comply with them to the best of my ability.

Ethical Data Usage:

Once you have completed training and signed your User Agreement, you are entitled to access to the Calgary HMIS. In addition to the responsibilities listed above, you must also adhere to the following principles of ethical data usage.

- Authorized Users will only ask Clients for information necessary to providing services, comply with contractual agreements, and to improve or better coordinate services;
- Authorized Users will ensure that Clients understand that their data is being collected and managed in the HMIS using the FOIP Verbal Notification as a guideline;
- Authorized Users will obtain a signed Release of Information (ROI) form before sharing client data with an outside program/agency on the HMIS
- Authorized Users will maintain a copy of the ROI Form;
- Authorized Users will not knowingly enter false and/or misleading information into the HMIS;
- Authorized Users will only use data in accordance with the Privacy Policy; and
- The Calgary Homeless Foundation, Participating Agencies, and Authorized Users will adhere to the HMIS Privacy Policy.

By affixing my signature to this document, I acknowledge that I have been apprised of the Calgary HMIS Policies and Standard Operating Procedures concerning access, use, maintenance, and disclosure of confidential information and/or records that shall be made available to me through my use or the Calgary HMIS.

_____

User Signature   Date

_____

Agency Contact Signature   Date

Appendix D: User License Fees

The following table provides the license fees for 2015:

License Type	Description	Cost Type	Cost of License (CDN)
User	Initial Purchase Fee	One Time	$240.00
User	Fee for maintenance, product enhancements and version upgrades	Annual	$81.00
ART	Maintenance Fee	Annual	$120.00

As these fees may vary from year to year, this document will be updated annually to reflect the change in fees (if any).

Complimentary Services

With the annual fee you also receive complimentary:

- Unlimited Training - Includes but not limited to: Basic to advanced software utilization, report training, ART, administrator training.

- Unlimited Support Service – Access to the HMIS team during business hours

How many user licenses do I need?

To ensure privacy and security, every HMIS user must have their own user license. If there are five people at your agency who need to log on to HMIS, then you must have five user licenses and each user must complete training and sign the User Agreement form.

Sharing of HMIS user licenses is strictly prohibited. Failure to comply not only compromises security, but is also a violation of federal privacy law. The HMIS staff can help you determine the exact number as part of the implementation.

THIS AGENCY PARTICIPATES IN THE CALGARY HOMELESS MANAGEMENT INFORMATION SYSTEM (HMIS)

We collect personal information directly from you that we consider to be important and necessary. We are required to collect some personal information by organizations that give us money to operate this program. Other personal information that we collect is important to provide you appropriate services, to run our programs, to improve services for homeless persons throughout Calgary, and to better understand the needs of persons who are experiencing homelessness or unstable housing situations. This information is entered into an electronic system called the Calgary Homeless Management Information System, also known as the Calgary HMIS.

The collection and use of all personal information is guided by strict standards of confidentiality. The [Agency Name] and all agencies accessing the Calgary HMIS follow policies within the Calgary Homeless Management Information System: Policies and Standard Operating Procedures.

A copy of our HMIS Privacy Policy and an HMIS Brochure describing our privacy practices and your rights are available upon request.

Appendix F: User Roles and Access Levels

Job Title	User Role	Type of Access (Read, Write, Edit)	Description of Information Visible to User
Vendor System Administrator	System Administrator	Read, write and edit access throughout the system	All information including Client identifiable information and Agency-specific information
HMIS Team	System Administrator	read, write and edit access throughout the system	All information including Client identifiable information and Agency-specific information
Executive Director	Administers Agency-specific information; able to audit Agency User access; able to enter and view Client information	Read, write and edit access at Agency-level only (Agency and any associated programs)	User can access all Agency profile information (necessary for Agency setup), User information, and Client information that has been input by any User within the Agency or that has been specifically shared with the Agency. Can delete Agency Administrator account
Agency Administrator	Administers agency-specific information; able to audit agency User access; able to enter and view Client information	Read, write and edit access at Agency-level only (Agency and any associated programs)	User can access all Agency profile information (necessary for Agency setup), User information, and Client information that has been input by any User within the Agency or that has been specifically shared with the Agency.
Case Manager	Enters and updates Client information necessary for the case management process	Read, write and edit access at the program-level only	User can access all Client files that are created or updated by the programs to which the User has been given access; User will manage assessments, case notes, referrals, and service information.
Agency Staff	Enters and updates Client information necessary for the case management process	Read, write and edit access at the program-level only	User can access all Client demographic information within the files that are created or updated by the programs to which the User has been given access; User will manage Client demographic, services provided and service records.

Appendix G: Client Grievance Form

Privacy Grievance Form
CALGARY HOMELESS MANAGEMENT INFORMATION SYSTEM (HMIS)

If you have complaints about <mark><Agency Name></mark>'s protection or use of your personal information in the HMIS, you can submit your grievance verbally or in writing by submitting this form to the HMIS Program Manager at the Calgary Homeless Foundation, 308-925 7 Avenue Southwest, Calgary, AB T2P 1A5, Canada. <mark><Agency Name></mark> will not deny services to you or your household members for submitting this grievance form.

Date: _____   Date of Incident: _____

Client Name (Print)

What happened?

Do you want to be contacted about the results? ☐ Yes   <u>or</u>   ☐ No.

If yes, how may we contact you?

Phone: _____   Email: _____

Mailing Address:

   (Street)   (Postal Code)

For Calgary HMIS Use

Please describe how the problem was resolved: _____ _____ _____ _____ Agency Representative Name: _____ Signature: _____   Date: _____

Data Collection Policy and ServicePoint

Calgary Homeless Management Information System (HMIS)

A.   Introduction

The Calgary Homeless Foundation (CHF) has created this Homeless Management Information System (HMIS) Data Collection Policy in order to demonstrate our firm commitment to a fair and compliant data collection processes. The HMIS complies with the Alberta *Freedom of Information Protection of Privacy Act* (FOIP).

Agencies using the HMIS collect two types of information from clients accessing their programs or services:

(1)   Information that is mandatory for the agency's operation of their programs (the "Agency Mandated Information"); and

(2)   Information required by CHF for the agency to collect (the "CHF Mandated Information").

Agencies already have their own polices in relation to the collection of the Agency Mandated Information. Both those agency policies and this policy apply to the Agency Mandated Information.

This policy establishes procedures that must be used when collecting Agency Mandated Information and CHF Mandated Information from clients accessing programs or services. Specifically, this policy sets out the information gathering and dissemination practices for collecting personal data from clients, storing personal data in the HMIS, and sharing personal data between agencies, for all agencies utilizing the HMIS, both CHF funded and non-funded. It is important to be aware of the fact that the HMIS is one of many business tools for client data storage in the Calgary System of Care.

B.   Verbal notification of data collection

Effective November 1, 2013, agencies will use a verbal notification for data collection replacing the prior verbal notification. Written consent forms ("Release of Information (ROI) Forms) are still required to share collected personal information across various programs within the Agency or with external programs within the Calgary System of Care. Written consent is required for all clients participating in the Coordinated Access and Assessment program in addition to the FOIP verbal notification. Agencies will remain FOIP compliant so long as the following steps are taken:

1.   The agency shall only collect information if that information relates directly to and is necessary for an operating program or activity of the agency (section 33(c) of the FOIP Act);

2. When information is collected from a client, it shall be collected directly from the client who shall be verbally notified as to:

1. The purpose for which the information is collected;

2. The specific legal authority for the data collection (in this case s33(c) of the Act); and

3. The title, business address and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection. Below, is a prepared statement by the Government of Alberta, Ministry of Human Services, which must be read to clients before their data is entered into the HMIS:

> *This personal information is being collected under the authority of Section 33(c) of the Freedom of Information and Protection of Privacy ACT (the `FOIP`) and/or in accordance with any applicable agreements in place. All personal information collected during the registration process, during the course of the client`s stay, and for participation in any programs will be used to provide services and ensure a safe and secure environment for all our clients. It will be treated in accordance with the privacy provision of Part 2 of the FOIP. Limited information may also be provided to the Minister of Human Services for the purpose of carrying out programs, activities or policies under his administration (e.g. research, statistical analysis) or for receiving provincial and/or federal funding. If you have any additional questions or concerns, please contact the Agency Administrator.*

Agencies are to ensure that this statement is available and read to all clients by staff prior to collecting client data and/or entering client data into the HMIS.

C.   Special considerations: HMIS Data Collection Process

Anonymous Clients

Funded agencies with provincial and federal contracts with the CHF are no longer permitted to input anonymous clients into the HMIS. Clients at these agencies are benefiting from a government program and are being funded using public dollars, and therefore the government has a degree of responsibility to the public to be able to audit the program and prove that clients are being accounted for. If a client refuses to answer any of the Universal Data Elements (UDE's) or assessment questions required by the

Government of Alberta or the Federal Government, then the staff member must put "Declined to Answer" in the required fields.

Non-funded agencies will still be able to enter clients as anonymous at their own discretion, however they should consult with their funders first.

Aliases

Funded agencies should seek to obtain legal names only and avoid aliases whenever possible. However, the CHF and our funders recognize that client aliases can and will be used by funded agencies from time to time. Non-funded programs should consult with their funders first in relation to the use of aliases.

Intoxication and Mental Health Considerations

When serving clients who are unable to understand the verbal notification due to mental health issues or intoxication, only a client's name, basic demographics (age/gender/ ethnicity) and services received by the client (i.e. meals, shelter stays etc.) may be collected and input in the HMIS. This still allows agencies to keep track of all clients in their care at any given time for safety reasons, to de-duplicate clients for reporting purposes and to track and account for the various resources used to care for a client.

Once the client has stabilized and is able to understand the verbal notification, then further information such as case plans and assessment info may also be collected and input.

Note that the verbal notification will not be considered valid if read to a client who is unable to comprehend it. It is up to the case manager to use their informed judgment as to whether or not a client has the mental capacity to comprehend the verbal notification. If in doubt, do not collect any information further than demographics and services received by the client. Case managers may want to document that the client was unable to understand the notification in a log/case notes once the client has been entered into the HMIS.

D. Data Collection and Funder Requirements

Refusal to Accept the Verbal Notification of Data Collection

Agencies are required and have the authority to collect personal information for service provision. Data collected by agency staff is stored securely in the HMIS and is never shared without written client consent. Should a client still refuse to have their information collected after the FOIP notification has been read and discussed, the following processes will apply:

a) **CHF-Funded Agencies:**

    I.   Housing First Programs and all programs where funding is subject to contractual client target numbers:

        (1) If the client does not provide data elements (name, demographics, UDEs, and HF assessments), as per Human Services and Homeless Partnering Strategy mandate, they cannot participate in the program.

    II.   Shelter programs:

        (1) Where the client refuses to provide any information, CHF does not require a client to provide information to stay at a shelter. Clients are not turned away from a shelter if they refuse to provide their information. Agencies may have other policies or procedures in this regard.

    III. Coordinated Access & Assessment program:

        (1) Where the client refuses to provide identifying information, it should be communicated that this may inhibit the ability of participating CAA programs to work collaboratively on behalf of the client. Clients are not turned away from participating in the CAA program and can be entered anonymously.

b) **Non-Funded Agencies:**

    I.   If the client refuses to have their information collected and stored in the HMIS, it is at the agencies discretion to enter clients who refuse as "anonymous" or under an alias or pseudonym, unless otherwise directed by their funders.

CHF Funded Family Providers

The CHF recognizes the dynamic nature of families being served in Calgary's System of Care. In order to capture the complete picture and data set of the services family partner agencies are providing, the following data collection policies apply:

a) All Program Types:

    1. Client Record (First and Last name) and Demographics are required to be collected and entered on all members of the family being served by the Program;

    2. Universal Data Elements are required to be collected and entered in the Calgary HMIS for all family members 18 years of age or older; and

    3. All CHF Funded Family providers are required to complete the Households tab in ServicePoint.

b) Housing First (Rapid Rehousing, Supportive Housing, Permanent Supportive Housing):

    1. Assigned Housing First assessments are ***required to be entered for the Head of Household only***. Should the question pertain to the entire household, this is noted in the wording of the question and should be answered accordingly; and

    2. Should the Housing First Provider have the resources, the Housing First assessments can also be completed with any other household member that is aged 18 or older.

c) Emergency Shelter:

    1. The Human Services Emergency Shelter assessment is ***required to be completed for the Head of Household only***; and

    2. Should the Emergency Provider have the resources, the Emergency Shelter assessment can also be completed with any other household member that is aged 18 or older.

Housing First (Rapid Rehousing, Supportive Housing, Permanent Supportive Housing) Programs and Client Transfers

Effective April 1, 2015, all clients transferring between CHF-Funded Housing First providers must complete the Housing First Exit Interview prior to transfer. Upon transfer to the new Housing First Provider the client will begin Housing First assessments at Intake.

If the client has not moved to new physical housing, the move-in date can be reflected as the clients' new Program Entry date.

The Entry/Exit reason for leaving is to be answered as Transferred to Housing First Program.

When entering transfer client into the new Housing First Program, the Housing First Transfer Indicator is to be answered as "Yes".

ShelterPoint

All Housing First, Prevention and Emergency Shelter providers are required to enter all clients served into the appropriate ShelterPoint unit list.

E.   Monitoring

The HMIS Team will work with the HMIS Agency Admin to monitor agencies to ensure that:

1. Agency staff understand the requirement for collection of personal information at their agency;

2. Agency staff understand what verbal notification of data collection means;

3. The verbal notification of data collection is read to and understood by every client;

4. For clients who are intoxicated or who have mental health considerations, only name, demographics and services are initially collected. Any further data collection will only occur after stabilization; and

5. Breaches of this policy and of the FOIP Act are prevented.

Breaches

A breach of these procedures or of the FOIP Act by an agency shall be immediately reported to the CHF in writing by emailing to HMIS@calgaryhomeless.com and placing ATTN: HMIS MANAGER – FOIP BREACH in the Subject Line.

Appendix I: Optional Written FOIP Consent Form

FOIP Client Consent Form
Authorization to Enter Personal Information in the
CALGARY HOMELESS MANAGEMENT INFORMATION SYSTEM (HMIS)

The use of the Calgary HMIS to manage client information is subject to the protection of personal information provisions of the Freedom of Information and Protection of Privacy (FOIP) Act. A copy of the Calgary HMIS Privacy Policy and further reading describing the HMIS privacy practices is available upon client request.

Client Name (Print)   **Date**   **of**   **Birth**
(Month/Day/Year)

Dependent children, if any (first and last names and dates of birth) who are receiving services and for whom the parent is providing consent:

_____

_____

I UNDERSTAND THAT:
- My consent is voluntary, and that failure to provide consent will not result in any adverse decision about my rights, benefits or services.
- I may revoke this consent at any time, in writing, and have my record deleted.
- I may consent to the sharing of personal information on behalf of minor children for whom I have legal guardianship, or for other persons for whom I am a legal representative.
- This agency will never give out information about me/and or my dependents to anyone outside of this agency without my written consent, or as required by law through a court order.
- I have a right to see my HMIS record, ask for changes, and to have a copy of my record from this agency upon request.
- This consent will expire in 1 year from when I cease to receive services from this agency.

Select One:

☐ I do consent to the collection, storage and management of my personal information in the Calgary HMIS

_____   _____
_____

Signature of Client   Print Client's Full Name   Date
(Month/Day/Year)

_____   _____
_____

Signature of Witness   Print Witness's Full Name   Date
(Month/Day/Year)

OR

☐ I do consent to the use of my information <u>anonymously</u> (i.e. without disclosing my name) for the participation in the Calgary HMIS

_____   _____
_____

Signature of Client   Print Client's Full Name   Date
(Month/Day/Year)

_____   _____
_____

Signature of Witness   Print Witness's Full Name   Date
(Month/Day/Year)

FOIP DISCLAIMER

This personal information is being collected under the authority of Section 33(c) of the Freedom of Information and Protection of Privacy ACT (the `FOIP`) and/or in accordance with any applicable agreements in place. All personal information collected during the registration process, during the course of the client`s stay, and for participation in any programs will be used to provide services and ensure a safe and secure environment for all our clients. It will be treated in accordance with the privacy provision of Part 2 of the FOIP. Limited information may also be provided to the Minister of Human Services for the purpose of carrying out programs, activities or policies under his administration (e.g. research, statistical analysis) or for receiving provincial and/or federal funding. If you have any questions, contact {Service Provider's name and contact information}.

Statement of Use:

The Calgary Homeless Management Information System (HMIS) is a web based, electronic client management information system providing a standardized assessment of client needs, individualized service plans and service records. The Calgary community utilizes the HMIS to understand the nature of homelessness, develop policies and initiatives to address homelessness, and coordinate case management services. The HMIS is managed by the Calgary Homeless Foundation (CHF).
Personal information that is collected will be used only for the purpose of providing counseling and intervention services. Services will be delivered primarily by the service providers. Where services need to be delivered by extended service providers, information will only be disclosed to them with consent. Information will not be used for any other purpose, unless required by law, and will only be disclosed to external parties with the consent of the individual to whom it pertains.

Authority:

FOIP s.33(c), the personal information is being collected on behalf of the Government of Alberta Human Services or another FOIP public body, and it is necessary for the operation of homeless programs being delivered on behalf of those public bodies. This consent will expire 1 year after the client has ceased receiving services under this program.

Freedom of Information and Privacy Protection Act
Verbal Notification

The following notification **must** be read to and discussed with all clients:

> *This personal information is being collected under the authority of Section 33(c) of the Freedom of Information and Protection of Privacy ACT (the `FOIP`) and/or in accordance with any applicable agreements in place. All personal information collected during the registration process, during the course of the client`s stay, and for participation in any programs will be used to provide services and ensure a safe and secure environment for all our clients. It will be treated in accordance with the privacy provision of Part 2 of the FOIP. Limited information may also be provided to the Minister of Human Services for the purpose of carrying out programs, activities or policies under his administration (e.g. research, statistical analysis) or for receiving provincial and/or federal funding. If you have any additional questions or concerns, please contact the Agency Administrator.*

The full *Freedom of Information and Protection of Privacy Act* can be found here:

http://www.qp.alberta.ca/1266.cfm?page=F25.cfm&leg_type=Acts&isbncln=9780779762071

HMIS FOIP Breach Procedure

Name of Staff submitting FOIP Breach Form:

Position:

Date:

CHF FOIP Officer:

Checklist:	Summary:
What were the circumstances that led to the breach?	
Who was involved?	
What information was lost, accessed, altered, or destroyed (includes short term losses)?	
What risk is there as a result of the loss – e.g. was the information encrypted, etc.?	
Is there a need to alert Clients whose information may have been accessed?	

Were all Policies and Standard Operating Procedures in place and being followed?
Do the policies/practices need to be reviewed and enhanced?
Could the incident have been avoided?
Is there a risk of a repeat incident?
What measures need to be put in place to avoid further similar incidents?

Appendix L: Links to Relative Documents

Below you will find links to other documents that are referred to but not included in the preceding document:

Privacy Impact Assessment: http://calgaryhomeless.com/wp-content/uploads/2014/05/HMIS-Privacy-Impact-Assessment.pdf

Freedom of Information and Protection of Privacy Act: http://www.qp.alberta.ca/1266.cfm?page=F25.cfm&leg_type=Acts&isbncln=9780779762071

Health Information Act   http://www.qp.alberta.ca/1266.cfm?page=h05.cfm&leg_type=Acts&isbncln=9780779780921

Personal Information and Protection of Privacy Act   http://www.qp.alberta.ca/1266.cfm?page=P06P5.cfm&leg_type=Acts&isbncln=9780779784554