Vermont Statewide

ServicePoint &

Homeless Management Information System

Policies and Procedures

VT HMIS Advisory Board

in partnership with

Institute for Community Alliances

2016

Contents

1. Introduction

The Vermont Homeless Management Information System (HMIS) is a collaborative project of the two Vermont Continua of Care (CoC) – Balance of State, and Chittenden County – the Institute for Community Alliances (ICA), and participating Partner Agencies. Our HMIS is an internet-based database, called ServicePoint, which is used by homeless service organizations across Vermont to record and store client-level information about the numbers, characteristics and needs of homeless persons and those at risk of homelessness. Bowman Internet Systems administers the central server and HMIS software, and ICA administers user and agency licensing, training and compliance.

HMIS enables service providers to measure the effectiveness of their interventions and facilitate longitudinal analysis of service needs and gaps within the CoCs. Information that is gathered from consumers via interviews conducted by service providers is analyzed for an unduplicated count, aggregated (void of any identifying client level information) and made available to policy makers, service providers, advocates, and consumer representatives. Data aggregated from HMIS about the extent and nature of homelessness in the state of Vermont is used to inform public policy decisions aimed at addressing and ending homelessness at local, state and federal levels.

Guidance for the implementation of Vermont's HMIS is provided by a broad-based advisory board that is committed to understanding the gaps in services to consumers of the human service delivery system in an attempt to end homelessness.

This document provides the policies, procedures, guidelines and standards that govern HMIS operations, as well as the responsibilities for Agency Administrators and end users.

1.1 HMIS BENEFITS

Use of HMIS provides numerous benefits for service providers, homeless persons and the State of Vermont.

Benefits for service providers

- Better able to define and understand the extent of homelessness throughout Vermont.
- Provides online real-time information about client needs and the services available for homeless persons.
- Assures confidentiality by providing information in a secured system.
- Decreases duplicative client intakes and assessments of shared files.
- Tracks client outcomes and provides a client history.
- Generates data reports for local use and for state and federal reporting requirements.
- Facilitates the coordination of services within an organization and, when data are shared, with other agencies and programs.
- Provides access to a statewide database of service providers, allowing agency staff to easily select a referral agency when data are shared.
- Better able to focus staff and financial resources where services for homeless persons are needed the most.

- Better able to evaluate the effectiveness of specific interventions and programs, and services provided.

Benefits for homeless persons

- Intake information and needs assessments are maintained historically, reducing the number of times homeless persons must repeat their stories to multiple service providers when data are shared.
- The opportunity to provide intake and life history one time demonstrates that service providers consider the homeless person's time valuable, and restores some of the consumer's dignity.
- Multiple services can be easily coordinated and referrals streamlined when data are shared.

2. Requirements for Participation

2.1 RESPONSIBILITIES OF HMIS USERS

Agency Administrators

1. Edit and update agency information in HMIS.
2. Ensure that the participating agency obtains a unique user license for each user at the agency.
3. Establish the standard report for each specific program created.
4. Maintain a minimum standard of data quality by ensuring the Universal Data Elements are complete and accurate for every individual served by the agency and entered into HMIS.
5. Maintain the required universal data elements and program specific data elements for each program in accordance with the current HMIS Data Standards, and maintain data elements required by the HMIS Advisory Board and/or the CoC in which the program operates.
6. Ensure agency staff persons receive required HMIS training, and review the Vermont HMIS Policies and Procedures, the Agency Partnership Agreement and any agency policies which impact the security and integrity of client information.
7. Ensure that HMIS access is granted only to staff members that have received both basic and security training, have completed the Vermont User Agreement and are authorized to use HMIS.
8. Notify all users at their agency of interruptions in service.
9. Provide a single point of communication between users and HMIS staff at the Institute for Community Alliances.
10. Administer and monitor data security policies and standards, including:
    - User access control;
    - The backup and recovery of data; and
    - Detecting and responding to violations of the policies and procedures or agency procedures.

Users

1. Take appropriate measures to prevent unauthorized data disclosure.
2. Report any security violations.
3. Comply with relevant policies and procedures.
4. Input required data fields in a current and timely manner. (Best practice is within 5 days with up to 30 days grace period.)
5. Ensure a minimum standard of data quality by accurately answering the Universal Data Elements and required program specific data elements for every individual entered into HMIS.
6. Inform clients about the agency's use of HMIS.
7. Take responsibility for any actions undertaken with one's username and password.
8. Complete required training.
9. Read the Vermont HMIS News email newsletter.

2.2 PARTNER AGENCY REQUIREMENTS

Participation Agreement Documents

Partner Agencies must complete the following documents:

1. **Partnership Agreements** must be signed by each participating agency's executive director or authorized representative. The Institute for Community Alliances will retain the original document. The participation agreement states the agency's commitment to adhere to the policies and procedures for effective use of HMIS.

2. **Vermont User Agreements** list user policies and responsibilities and are electronically signed by each authorized user. An electronic or hard copy of the original document must be kept by the originating agency.

3. **Coordinated Services Agreements** allow the specifically named HMIS user to enter client data as, or on behalf of, another specifically named Participating Agency and/or to report on behalf the specifically named Participating Agency. The signed agreement will be maintained by the HMIS Lead Agency, the Institute for Community Alliances.

User Access to the System

The Agency Administrator will determine user access for users at or below the Case Manager III access level and assign users to the appropriate agency provider. The System Administrator will generate usernames and passwords within the administrative function of the software.

The Agency Administrator and all users must complete training before access to the system is granted by ICA. It is recommended that all users undergo a criminal background check as detailed in the Agency Partnership Agreement at this time, pending HMIS Final Rule.

User Requirements

Users must be paid staff or official volunteers of a Partner Agency. An official volunteer must complete a volunteer application with the Partner Agency, undergo agency training, pass a criminal background check, and record volunteer hours with the agency. Individuals who are solely contracting with a Partner Agency are prohibited from receiving a user license. All users must be at least 18 years old.

Users who are also Clients Listed in HMIS

In order to prevent users from editing their own file or files of immediate family members, all users will agree to a conflict of interest statement that is part of the User Agreement. Users must disclose any potential conflict of interest to their Agency Administrator. Users will be prohibited from making changes to the information in their own file or the files of their immediate family members. If a user is suspected of violating this agreement, the System Administrator will run the audit trail report to determine if there was an infraction.

Passwords

- Creation: Passwords are automatically generated from the system when a user is created. The System Administrator or Agency Administrator will communicate the system-generated password to the user.
- Use: The user will be required to change the password the first time they log onto the system. The password must be at least 8 characters and alphanumeric. Passwords

should not be able to be easily guessed or found in a dictionary. Passwords are the individual's responsibility and users cannot share passwords. Users may not keep written copies of their password in a publicly accessible location.

- Storage: Any passwords that are written down are to be stored securely and must be inaccessible to other persons. Users are not to store passwords on a personal computer for easier log on.
- Expiration: Passwords expire every 45 days. Users may not use the same password consecutively. Passwords cannot be re-used until 2 password selections have expired.
- Unsuccessful logon: If a user unsuccessfully attempts to log-on 3 times, the User ID will be "locked out," and access permission will be revoked rendering the user unable to gain access until his/her password is reset.

Inputting Data

Agencies participating in the HMIS must meet the minimum data entry requirements established by the current HMIS Data Standards.

Tracking of Unauthorized Access

Any suspicion of unauthorized activity should be reported to the Institute for Community Alliances HMIS staff.

Agency Administrator

Agencies with 10 or more users must designate one person to be the Agency Administrator. Agencies with fewer than 10 users may forego designating an Agency Administrator. ICA HMIS staff will perform Agency Administrator responsibilities for these agencies.

The Agency Administrator, or System Administrator when no Agency Administrator is designated, will be responsible for resetting passwords, and monitoring HMIS access by users at their agency. This person will also be responsible for ensuring new agency staff persons are trained on how to use the HMIS by the System Administrators and for ensuring that new staff are aware of any agency or program specific data entry requirements.

The Agency Administrator must identify the assessments and requirements for each program, and work with the System Administrators to properly set up each program in the HMIS.

Client Consent for Sharing Data Forms

In addition to posting the HMIS Consumer Notice, agencies are required to have clients sign a client consent form if the client's data are shared in the system. The form requires clients to authorize the electronic sharing of their personal information with other agencies that participate in HMIS when data sharing is appropriate for client service.

Data Protocols

Agencies may collect information for data elements in addition to the minimally required data elements established by the HMIS Advisory Board in accordance with HUD. Agencies must maintain consistency with data collection and entry within each program.

2.4 USER TRAINING REQUIREMENTS

New User Training Requirements

All users are required to attend new user training with ICA prior to receiving access to the system. If ICA determines that data entered by a current end user does not meet minimum data quality standards, users may be required to repeat this training.

Once a new user begins the HMIS new user training series, the user has 15 days to complete the training series and all required assignments. ICA staff will review the user's homework and determine if corrections are needed. Users will have an additional 15 days to make all corrections. If the user fails to complete all requirements within 30 days, the user will need to retake the training series. ICA staff may determine that a new user failed to grasp the necessary data entry concepts based on the quality of the user's homework. ICA staff may use their discretion to require new users to repeat new user training. If a new user fails to successfully complete the homework requirements for data entry after repeated attempts, ICA staff may use their discretion to determine that the new user is not capable of accurate and complete data entry, and may refuse to issue the new user a Vermont HMIS user license.

If a user requesting a new user license had a license for the Vermont HMIS in the past, the user will be required to re-take the training series, with few exceptions. ICA has sole discretion to waive the requirement to attend new user training. ICA will consider the user's familiarity with the HMIS and the need for the user to learn about potential system updates and changes during new user training when making its decision to waive the new user training requirement.

Users are expected to fully participate in all trainings attended. If a user misses more than ten minutes or ten percent (whichever is greater) of a training, the user will not receive credit for completing the training.

Ongoing User Training Requirements

All users are required to attend annual security training to retain their user license.

All users are required to attend at least two general HMIS trainings annually. The new user training series will count as one training toward the general training requirement. New users taking the new user training series in December will be exempt from completing an additional training during that calendar year.

All users with Advanced Reporting Tool (ART) Licenses are required to attend at least two ART trainings annually in addition to the required general HMIS trainings.

Users are expected to fully participate in all trainings attended. If a user misses more than ten minutes or ten percent (whichever is greater) of a training, the user will not receive credit for completing the training.

2.5 HMIS USER LEVELS

HMIS user roles are listed on the ICA website.

Resource Specialist I
Users at this level may access only the ResourcePoint module. Users may search the database of area agencies and programs, and view the agency or program detail screens. A Resource Specialist I cannot modify or delete data, and does not have access to client or service records or other modules and screens.

Resource Specialist II
Users may access only the ResourcePoint module. Users may search the database of area agencies and programs, and view the agency or program detail screens. At this level, the user does not have access to client or service records or other modules and screens. A Resource Specialist II is an agency-level "Information & Referral (I&R) specialist" who may update their own agency and program information.

Resource Specialist III
Users at this level may access only the ResourcePoint module. Users may search the database of area agencies and programs and view the agency or program detail screens. A Resource Specialist III may add or remove resource groups, including Global (which they get by default). Access to client or service records and other modules and screens is not given. A Resource Specialist III may edit the system-wide news feature.

Volunteer
Users may access ResourcePoint, and have limited access to ClientPoint and service records. A volunteer may view or edit basic demographic information about clients (the profile screen), but is restricted from all other screens in ClientPoint. A volunteer may also enter new clients, make referrals, and check clients in/out from a shelter. A volunteer does not have access to the "Services Provided" tab. This access level is designed to allow a volunteer to perform basic intake steps with a new client and then refer the client to an agency staff member or case manager.

Agency Staff
Users may access ResourcePoint, have full access to service records, and limited access to ClientPoint. Agency staff may access most functions in ServicePoint, however, they may only access basic demographic data on clients (profile screen). All other screens are restricted including Reports. Agency Staff can add news items to the newswire feature.

Case Manager I
Users may access all screens and modules except "Administration." A Case Manager I may access all screens within ClientPoint, except the medical screen for confidentiality reasons. Users may access Reports.

Case Manager II
Users may access all screens and modules except "Administration." A Case Manager II may access all screens within ClientPoint, including the medical screen. Users may access Reports.

Case Manager III
This role has the same actions available as the Case Manager II with the added ability to see program data for all providers on their provider tree, like an Agency Administrator.

Agency Administrator

Users may access all ServicePoint screens and modules. Agency Administrators may add/remove users and edit agency and program data for all providers on their provider tree.

Executive Director
Users have the same access rights as an Agency Administrator, but rank above the Agency Administrator.

System Operator
Users may only access Administration screens. System operators can create new agency providers, add new users, reset passwords, and access other system-level options. Users may order additional user licenses and modify the allocation of licenses. They maintain the system, but may not access any client or service records.

System Administrator I
Users have the same access rights to client information as Agency Administrators, but for all agencies in the system. System Administrators also have full access to administrative functions.

System Administrator II
There are no system restrictions on users. They have full HMIS access.

2.6 HMIS VENDOR REQUIREMENTS

Physical Security
Access to areas containing HMIS equipment, data and software will be secured.

Firewall Protection
The vendor will secure the perimeter of its network using technology from firewall vendors. Company system administrators monitor firewall logs to determine unusual patterns and possible system vulnerabilities.

User Authentication
Users may only access HMIS with a valid username and password combination that is encrypted via SSL for internet transmission to prevent theft. If a user enters an invalid password three consecutive times, they are automatically shut out of that HMIS session. For added security, the session key is automatically scrambled and re-established in the background at regular intervals.

Application Security
HMIS users will be assigned a system access level that restricts their access to appropriate data.

Database Security
Wherever possible, all database access is controlled at the operating system and database connection level for additional security. Access to production databases is limited to a minimal number of points; as with production servers, production databases do not share a master password database.

Technical Support
The vendor will assist ICA HMIS staff to resolve software problems, make necessary modifications for special programming, and will explain system functionality to ICA.

Technical Performance
The vendor maintains the system, including data backup, data retrieval and server functionality/operation. Upgrades to the system software will be continuously developed and implemented.

Hardware Disposal
Data stored on broken equipment or equipment intended for disposal will be destroyed using industry standard procedures.

2.7 MINIMUM TECHNICAL STANDARDS

Minimum Computer Requirements

- A PC with a 2 Gigahertz or higher processor, 40GB hard drive, 512 MB RAM, and Microsoft Windows 7 or 8
- The most recent version of Google Chrome, Safari or Firefox. No additional plug-in is required.
  It is recommended that your browser have a 128 cipher / encryption strength installed.
  The browser's cache should be set to "Check for new version of the stored pages: Every visit to page."
- A broadband Internet connection or LAN connection. Dial-up modem connections are not sufficient.
- Virus protection updates
- Mobile devices used for HMIS data entry must use the Mozilla Firefox, Google Chrome or Apple Safari internet browsers. Apple Safari must be used on the latest version of iOS.

Additional Recommendations

Memory
- Windows 7: 4Gig recommended (2 Gig minimum)

Monitor
- Screen Display: 1024x768 (XGA) or higher; 1280x768 strongly advised

Processor
- A Dual-Core processor is recommended

2.8 HMIS LICENSE FEES

Annual Vermont HMIS License Fees
Agencies may purchase licenses at any time. The amount of a user license may change depending on the operating costs of the Vermont HMIS. All changes in amounts charged for user licenses will be approved by the HMIS Advisory Board.

Billing for licenses will occur once annually in January, covering January - December. The annual fee will cover the subsequent calendar year and must be paid within 60 days following the date of the invoice. If a Partner Agency fails to pay their license fees by the stated due date, the agency's user licenses will be suspended until ICA receives the payment.

Non-use Fee

Agencies with users who do not access their HMIS account at least once every 90 days will be assessed a Non-use Fee. For each user who does not meet the access requirement, the agency will be charged $500 at the time of annual license renewal. Participating Agencies are responsible for monitoring staff use of the HMIS to ensure that their agency is not charged Non-use Fee.

Fees for Programs Mandated to Use HMIS

Funding shall be provided from agencies operating programs required by federal and state agencies to enter data into HMIS as needed to fully fund the operation of the HMIS. The amount charged will be a set dollar amount or a percentage allocation of the funding source, to be determined by ICA based upon various criteria.

ART Licenses

The ART license is an add-on license available for HMIS users to facilitate data reporting. The additional amount charged for these licenses will reflect the actual cost of the license charged to the HMIS Lead Agency under the HMIS software contract.

2.9 HMIS OPERATING POLICIES VIOLATION

HMIS users and Partner Agencies must abide by all HMIS operational policies and procedures found in the HMIS Policies and Procedures manual, the Vermont User Agreement, and the Partner Agency Agreement. Repercussion for any violation will be assessed in a tiered manner. Each user or Partner Agency violation will face successive consequences – the violations do not need to be of the same type in order to be considered second or third violations. User violations do not expire. No regard is given to the duration of time that occurs between successive violations of the HMIS operation policies and procedures as it relates to corrective action.

- First Violation – the user and Partner Agency will be notified of the violation in writing by ICA. The user's license will be suspended for 30 days, or until the Partner Agency notifies ICA of action taken to remedy the violation. ICA will provide necessary training to the user and/or Partner Agency to ensure the violation does not continue. ICA will notify the HMIS Advisory Board of the violation during the next scheduled Advisory Board meeting following the violation.

- Second Violation – the user and Partner Agency will be notified of the violation in writing by ICA. The user's license will be suspended for 30 days. The user and/or Partner Agency must take action to remedy the violation; however, this action will not shorten the length of the license suspension. If the violation has not been remedied by the end of the 30-day user license suspension, the suspension will continue until the Partner Agency notifies ICA of the action taken to remedy the violation. ICA will provide necessary training to the user and/or Partner Agency to ensure the violation does not continue. ICA will notify the HMIS Advisory Board of the violation during the next scheduled Advisory Board meeting following the violation.

- Third Violation – the user and Partner Agency will be notified of the violation in writing by ICA. ICA will notify the HMIS Advisory Board of the violation and convene a review panel made up of Advisory Board members who will determine if the user's license should be terminated. The user's license will be suspended for a minimum of 30 days, or until the

Advisory Board review panel notifies ICA of their determination, whichever occurs later. If the Advisory Board determines the user should retain their user license, ICA will provide necessary training to the user and/or Partner Agency to ensure the violation does not continue. If users who retain their license after their third violation have an additional violation, that violation will be reviewed by the Advisory Board review panel.

Any user or other fees paid by the Partner Agency will not be returned if a user's or Partner Agency's access to HMIS is revoked.

Notifying the HMIS Lead Agency of a Violation

It is the responsibility of the Agency Administrator or general User at Partner Agencies that do not have an agency administrator to notify the HMIS Lead Agency when they suspect that a User or Partner Agency has violated any HMIS operational agreement, policy or procedure. A complaint about a potential violation must include the User and Partner Agency name, and a description of the violation, including the date or timeframe of the suspected violation. Complaints should be sent in writing to the HMIS Lead Agency at VTHMIS@icalliances.org. The name of the person making the complaint will not be released from the HMIS Lead Agency if the individual wishes to remain anonymous.

Violations of Local, State or Federal Law

Any Partner Agency or user violation of local, state or federal law will immediately be subject to the consequences listed under the Third Violation above.

Multiple Violations within a 12-Month Timeframe

During a 12 month calendar year, if there are multiple users (3 or more) with multiple violations (2 or more) from one Partner Agency, the Partner Agency as a whole will be subject to the consequences listed under the Third Violation above.

3. Privacy and Security

The importance of the integrity and security of HMIS cannot be overstated. Given this importance, HMIS must be administered and operated under high standards of data privacy and security. The Institute for Community Alliances and Partner Agencies are jointly responsible for ensuring that HMIS data processing capabilities, including the collection, maintenance, use, disclosure, transmission and destruction of data, comply with the HMIS privacy, security and confidentiality policies and procedures. When a privacy or security standard conflicts with other Federal, state and local laws to which the Partner Agency must adhere, the Partner Agency must contact ICA to collaboratively update the applicable policies for the partner agency to accurately reflect the additional protections.

3.1 DATA ASSESSMENT AND ACCESS

All HMIS data will be handled according to the following major classifications: Shared or Not Shared Data. HMIS staff will assess all data, and implement appropriate controls to ensure that data classified as shared or not shared are handled according to the following procedures.

Shared Data
Shared data is unrestricted information that has been entered by one provider and is visible to other providers using HMIS. Vermont's HMIS is designed as a Not Shared system that defaults to not sharing data. Providers have the option of changing their program settings to share client data not shared.

Data that is Not Shared
Information entered by one provider that is not visible to other providers using HMIS. Programs that serve victims of domestic violence, individuals with HIV/AIDS, provide youth services, or legal services must enter closed data. Further, programs that provide youth services and legal services may enter clients as "unnamed." Individual client records can be closed at the client's request.

Procedures for transmission and storage of data

- Open Data: This is data that does not contain personal identifying information. The data should be handled discretely, unless it is further classified as Public Data. The data must be stored out of site, and may be transmitted via internal or first-class mail until it is considered public data.
- Confidential Data at the Agency Level: Confidential data contains personal identifying information. Each agency shall develop rules governing the access of confidential data in HMIS to ensure that those staff needing confidential data access will have access, and access is otherwise restricted. The agency rules shall also cover the destruction of paper and electronic data in a manner that will ensure that privacy is maintained and that proper controls are in place for any hard copy and electronic data that is based on HMIS data.

Whenever confidential data is accessed:

- Hard copies shall be shredded when disposal is appropriate. Hard copies shall be stored in a secure environment that is inaccessible to the general public or staff not requiring access.
- Hard copies shall not be left out in the open or unattended.

- Electronic copies shall be stored only where the employee can access the data.
- Electronic copies shall be stored where a password is required to access the data if on shared server space.

All public data must be classified as aggregated public or unpublished restricted access data.

Aggregated Public Data
Information published according to the "Reporting Parameters and Guidelines" (HMIS Policies and Procedures Section 3.2).

Unpublished Restricted Access Data
Information scheduled, but not yet approved, for publication. Examples include draft reports, fragments of data sets, and data without context or data that have not been analyzed.

Procedures for Transmission and Storage of Data
- Aggregated Public Data: Security controls are not required.
- Unpublished Restricted Access Data:
    1. Draft or Fragmented Data – Accessible only to authorized HMIS staff and agency personnel. Requires auditing of access and must be stored in a secure out-of-sight location. Data can be transmitted via e-mail, internal departmental or first class mail. If mailed, data must be labeled confidential.
    2. Confidential Data: Requires encryption at all times. Must be magnetically overwritten and destroyed. Hard copies of data must be stored in an out-of-sight secure location.

3.2 DATA REPORTING PARAMETERS AND GUIDELINES

All open data will be handled according to the following classifications - *Public Data*, *Internal Data, and Restricted Data* - and should be handled according to the following procedures.

Principles for Release of Data
- Only de-identified aggregated data will be released except as specified below.
- No identified client data may be released without informed consent unless otherwise specified by Vermont State and Federal confidentiality laws. All requests for such information must be addressed to the owner/participating agency where the data was collected.
- Program specific information used for annual grant program reports and program specific information included in grant applications is classified as public information. No other program specific information will be released without written consent.
- There will be full access to aggregate data included in published reports.
- Reports of aggregate data may be made directly available to the public.
- The parameters of the aggregated data, that is, where the data comes from and what it includes will be presented with each report.
- Data will be mined for agencies requesting reports on a case-by-case basis.
- Requests must be written with a description of specific data to be included and for what duration of time. Requests are to be submitted at least 30 days prior to the date the report is needed. Exceptions to the 30-day notice may be made.
- ICA reserves the right to deny any request for aggregated data.

3.3 RELEASE OF DATA FOR GRANT FUNDERS

Entities providing funding to agencies or programs required to use HMIS will not have automatic access to HMIS. Access to HMIS will only be granted by ICA when there is a voluntary written agreement in place between the funding entity and the agency or program. Funding for any agency or program using HMIS cannot be contingent upon establishing a voluntary written agreement allowing the funder HMIS access.

3.4 BASELINE PRIVACY POLICY

Collection of Personal Information

Personal information will be collected for HMIS only when it is needed to provide services, when it is needed for another specific purpose of the agency where a client is receiving services, or when it is required by law. Personal information may be collected for these purposes:

- To provide or coordinate services for clients
- To find programs that may provide additional client assistance
- To comply with government and grant reporting obligations
- To assess the state of homelessness in the community, and to assess the condition and availability of affordable housing to better target services and resources

Only lawful and fair means are used to collect personal information.

Personal information is collected with the knowledge and consent of clients. It is assumed that clients consent to the collection their personal information as described in this notice when they seek assistance from an agency using HMIS and provide the agency with their personal information.

If an agency reasonably believes that a client is a victim of abuse, neglect or domestic violence, or if a client reports that he/she is a victim of abuse, neglect or domestic violence, explicit permission is required to enter and share the client's information in HMIS.

Personal information may also be collected from:

- Additional individuals seeking services with a client
- Other private organizations that provide services and participate in HMIS

Upon request, clients must be able to access the *Use and Disclosure of Personal Information* policy found below.

Use and Disclosure of Personal Information

These policies explain why an agency collects personal information from clients. Personal information may be used or disclosed for activities described in this part of the notice. Client consent to the use or disclosure of personal information for the purposes described in this notice, and for reasons that are compatible with purposes described in this notice but not listed, is assumed. Clients must give consent before their personal information is used or disclosed for any purpose not described here.

Personal information may be used or disclosed for the following purposes:

1. *To provide or coordinate services to individuals. Client records are shared with other organizations that may have separate privacy policies and that may allow different uses and disclosures of the information. If clients access services at one of these other*

organizations, they will be notified of the agency's privacy and sharing policy. {OPTIONAL}

2. To carry out administrative functions such as legal audits, personnel, oversight, and management functions.

3. For research and statistical purposes. Personal information released for research and statistical purposes will be anonymous.

4. For academic research conducted by an individual or institution that has a formal relationship with the Institute for Community Alliances. The research must be conducted by an individual employed by or affiliated with the organization or institution. All research projects must be conducted under a written research agreement approved in writing by the designated agency administrator or executive director. The written research agreement must:
    - Establish the rules and limitations for processing personal information and providing security for personal information in the course of the research.
    - Provide for the return or proper disposal of all personal information at the conclusion of the research.
    - Restrict additional use or disclosure of personal information, except where required by law.
    - Require that the recipient of the personal information formally agree to comply with all terms and conditions of the written research agreement, and
    - Be substituted, when appropriate, by Institutional Review Board, Privacy Board or other applicable human subjects' protection institution approval.

5. When required by law. Personal information will be released to the extent that use or disclosure complies with the requirements of the law.

6. For a law enforcement purpose (if consistent with applicable law and standards of ethical conduct) under any of these circumstances:

    - In response to a lawful court order, court-ordered warrant, subpoena or summons issued by a judicial officer or a grand jury subpoena, if the court ordered disclosure goes through the Institute for Community Alliances and is reviewed by the Executive Director for any additional action or comment.
    - If the law enforcement official makes a written request for personal information. The written request must meet the following requirements:
        i. Be signed by a supervisory official of the law enforcement agency seeking the personal information.
        ii. State how the information is relevant and material to a legitimate law enforcement investigation.
        iii. Identify the personal information sought.
        iv. Be specific and limited in scope to the purpose for which the information is sought, and
        v. Be approved for release by the Institute for Community Alliances legal counsel after a review period of seven to fourteen days.
    - If it is believed that the personal information constitutes evidence of criminal conduct that occurred at the agency where the client receives services.

- If the official is an authorized federal official seeking personal information for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to a foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 (threats against the President and others), and the information requested is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought.

7. For law enforcement or another public official authorized to receive a client's personal information to conduct an immediate enforcement activity that depends upon the disclosure. Personal information may be disclosed when a client is incapacitated and unable to agree to the disclosure if waiting until the individual is able to agree to the disclosure would materially and adversely affect the enforcement activity. In this case, the disclosure will only be made if it is not intended to be used against the individual.

8. To avert a serious threat to health or safety if:
    - the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public, and
    - the use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat.

9. To report to a governmental authority (including a social service or protective services agency) authorized by law to receive reports of abuse, neglect or domestic violence, information about an individual reasonably believed to be a victim of abuse, neglect or domestic violence. When the personal information of a victim of abuse, neglect or domestic violence is disclosed, the individual whose information has been released will promptly be informed, except if:
    - it is believed that informing the individual would place the individual at risk of serious harm, or
    - a personal representative (such as a family member or friend) who is responsible for the abuse, neglect or other injury is the individual who would be informed, and it is believed that informing the personal representative would not be in the best interest of the individual as determined in the exercise of professional judgment.

10. To comply with government reporting obligations for homeless management information systems and for oversight of compliance with homeless management information system requirements.

<u>Inspection and Correction of Personal Information</u>
Clients may inspect and receive a copy of their person information maintained in HMIS. The agency where the client receives services will offer to explain any information that a client may not understand.

If the information listed in HMIS is believed to be inaccurate or incomplete, a client may submit a verbal or written request to have his/her information corrected. Inaccurate or incomplete data may be deleted, or marked as inaccurate or incomplete and supplemented with additional information.

A request to inspect or copy one's personal information may be denied if:

- The information was compiled in reasonable anticipation of litigation or comparable proceedings
- The information was obtained under a promise or confidentiality and if the disclosure would reveal the source of the information, or
- The life or physical safety of any individual would be reasonably endangered by disclosure of the personal information.

If a request for inspection access or personal information correction is denied, the agency where the client receives services will explain the reason for the denial. The client's request and the reason for the denial will be included in the client's record.

Requests for inspection access or personal information correction may be denied if they are made in a repeated and/or harassing manner.

Limits on Collection of Personal Information
Only personal information relevant for the purpose(s) for which it will be used will be collected. Personal information must be accurate and complete.

Client files not used in seven years may be made inactive in HMIS. ICA will check with agencies before making client files inactive. Personal information may be retained for a longer period if required by statute, regulation, contract or another obligation.

Limits on Partner Agency Use of HMIS Client Information
The Vermont HMIS is an open data system. This system allows Partner Agencies to share client information in order to coordinate services for clients. However, Partner Agencies may not limit client service or refuse to provide service in a way that discriminates against clients based on information the Partner Agency obtained from HMIS. Partner Agencies may not penalize a client based on historical data contained in HMIS.

Youth providers serving clients under the age of 18 must maintain closed HMIS client files. Youth under the age of 18 may not provide either written or verbal consent to the release of their personally identifying information in HMIS.

Complaints and Accountability
Questions or complaints about the privacy and security policies and practices may be submitted to the agency where the client receives services. Complaints specific to HMIS should be submitted to the HMIS agency administrator and program director. If no resolution can be found, the complaint will be forwarded to the System Administrators, and the agency's executive director. If there is no resolution, the Vermont HMIS Advisory Board will oversee final arbitration. All other complaints will follow the agency's grievance procedure as outlined in the agency's handbook.

All HMIS users (including employees, volunteers, affiliates, contractors and associates) are required to comply with this privacy notice. Users must receive and acknowledge receipt of a copy of this privacy notice.

3.5 USE OF A COMPARABLE DATABASE BY VICTIM SERVICE PROVIDERS

Victim service providers, private nonprofit agencies whose primary mission is to provide services to victims of domestic violence, dating violence, sexual assault, or stalking, must not directly enter or provide data into HMIS if they are legally prohibited from participating in HMIS. Victim service providers that are recipients of funds requiring participation in HMIS, but are prohibited from entering data in HMIS, must use a comparable database to enter client information. A comparable database is a database that can be used to collect client-level data over time and generate unduplicated aggregated reports based on the client information entered into the database. The reports generated by a comparable database must be accurate and provide the same information as the reports generated by HMIS.

3.6 USER CONFLICT OF INTEREST

Users who are also clients with files in HMIS are prohibited from entering or editing information in their own file. All users are also prohibited from entering or editing information in files of immediate family members. All users must sign the Vermont User Agreement, which includes a statement describing this limitation, and report any potential conflict of interest to their Agency Administrator. The System Administrator may run the audit trail report to determine if there has been a violation of the conflict of interest agreement.

3.7 SECURITY PROCEDURE TRAINING FOR USERS

All users must receive security training prior to being given access to HMIS. Security training will be covered during the new user training for all new users. All users must receive ongoing annual training on security procedures from the Institute for Community Alliances.

3.8 VIOLATION OF SECURITY PROCEDURES

All potential violations of any security protocols will be investigated and any user found to be in violation of security protocols will be sanctioned accordingly. Sanctions may include but are not limited to: a formal letter of reprimand, suspension of system privileges, revocation of system privileges and criminal prosecution.

If possible, all confirmed security violations will be communicated in writing to the affected client within 14 days, unless the client cannot be located. If the client cannot be located, a written description of the violation and efforts to locate the client will be prepared by the System Administrator at the Institute for Community Alliances, and placed in the client's file at the Agency that originated the client's record.

Any agency that is found to have consistently and/or flagrantly violated security procedures may have their access privileges suspended or revoked. All sanctions are imposed by the ICA HMIS staff. All sanctions may be appealed to the HMIS Advisory Board.

3.9 PROCEDURE FOR REPORTING SECURITY INCIDENTS

Users and Agency Administrators should report all unlawful access of HMIS and unlawful attempted access of HMIS. This includes theft of usernames and passwords. Security incidents

should be reported to the ICA System Administrator. The ICA System Administrator will use the HMIS user audit trail report to determine the extent of the breach of security.

3.10 DISASTER RECOVERY PLAN

Bowman Systems Disaster Recovery Plan

Vermont's HMIS is covered under Bowman Systems Disaster Recovery Plan. Due to the nature of technology, unforeseen service outages may occur. In order to assure service reliability, Bowman Systems provides the following disaster recovery plan. Plan highlights include:

- Database tape backups occur nightly.
- Tape backups are stored offsite.
- Seven day backup history is stored locally on instantly accessible Raid 10 storage.
- One month backup history is stored off site.
- Access to Bowman Systems emergency line to provide assistance related to "outages" or "downtime" 24 hours a day.
- Data is backed up locally on instantly-accessible disk storage every 24 hours.
- The application server is backed up offsite, out-of-state, on a different internet provider and on a separate electrical grid via secured Virtual Private Network (VPN) connection.
- Backups of the application site are near-instantaneous (no files older than 5 minutes).
- The database is replicated nightly at an offsite location in case of a primary data center failure.
- Priority level response (ensures downtime will not exceed 4 hours).

Standard Data Recovery

Vermont's HMIS database is stored online, and is readily accessible for approximately 24 hours a day. Tape backups of the database are kept for approximately one month. Upon recognition of a system failure, HMIS can be copied to a standby server. The database can be restored, and the site recreated within three to four hours if online backups are accessible. As a rule, a tape restoration can be made within six to eight hours. On-site backups are made once daily. A restore of this backup may incur some data loss between when the backup was made and when the system failure occurred.

All internal servers are configured in hot-swappable hard drive RAID configurations. All systems are configured with hot-swappable redundant power supply units. Our Internet connectivity is comprised of a primary and secondary connection with separate internet service providers to ensure redundancy in the event of an ISP connectivity outage. The primary Core routers are configured with redundant power supplies, and are configured in tandem so that if one core router fails the secondary router will continue operation with little to no interruption in service. All servers, network devices, and related hardware are powered via APC Battery Backup units that are connected in turn to electrical circuits, which are connected to a building generator.

All client data is backed-up online and stored on a central file server repository for 24 hours. Each night a tape backup is made of the client database and secured in a bank vault.

Historical data can be restored from tape as long as the data requested is newer than 30 days old. As a rule, the data can be restored to a standby server within four hours without affecting the current live site. Data can then be selectively queried and/or restored to the live site.

For power outage, HMIS is backed up via APC battery back-up units, which are connected via generator-backed up electrical circuits. For a system crash, a system restore will take four

hours. There is potential for some small data loss (data that was entered between the last backup and when the failure occurred) if a tape restore is necessary. If the failure is not hard drive related, the data restore time will possibly be shorter as the drives themselves can be repopulated into a standby server.

All major outages are immediately brought to the attention of executive management. Bowman Systems support staff helps manage communication or messaging to the System Administrator as progress is made to address the service outage.

Vermont HMIS Disaster Recovery Plan

The Institute for Community Alliances operates a regional approach to administering the Vermont HMIS. The main ICA Vermont HMIS office is in Madison, WI, a secondary office in Green Bay, WI, and an office located in the state of Vermont. In the event of a localized emergency or disaster, ICA will shift responsibility for administering the HMIS and managing day-to-day operations of the system to an unaffected site.

4. Data Requirements

4.1 MINIMUM DATA COLLECTION STANDARD

Partner Agencies are responsible for asking all clients a minimum set of questions for use in aggregate analysis. These questions are included in custom assessments that are created by HMIS System Administrators. The required data elements depend on the program. The mandatory data elements in each assessment are displayed in *red* text and/or specific text indicating that the field is required.

The Agency Administrator must identify the assessments and requirements for each program. ICA will consult with the Agency Administrator to properly set up each program in HMIS.

Guidelines clearly articulating the minimum expectations for data entry for all programs entering data in HMIS will be sent to Agency Administrators and posted on the Institute for Community Alliances' Vermont HMIS webpage. Agency Administrators must ensure that the minimum data elements are fulfilled for every program.

4.2 PROVIDER NAMING CONVENTION

All providers within HMIS must be named so that they accurately reflect the type of service carried out by the corresponding Partner Agency program.

4.3 DATA QUALITY PLAN

Partner Agencies are responsible for the overall quality, accuracy and completeness of data entered by their staff for their clients. HMIS staff will monitor data collection of the HMIS Universal Data Elements and required program specific data elements monthly and hold participating agencies accountable for not entering required data.

ICA will submit a report to each CoC annually that identifies the degree to which all agencies within the CoC are meeting the minimum data entry standards.

Programs that do not adhere to the minimum data entry standards will be notified of their deficiencies and given appropriate training on how to correctly enter data. Partner Agencies and/or users who do not meet minimum data entry standards following additional training from ICA will be considered in violation of the HMIS operating agreements, and will be subject to the repercussions listed in Section 2.9 of the HMIS Policies and Procedures Manual.

4.4 XML IMPORTS

While HMIS vendors are required to have the capacity to accept CSV and/or XML imports per federal regulations, a CoC has at its discretion whether or not to permit imports and may require direct data entry into the CoC designated HMIS. The Balance of State CoC and the Chittenden/Burlington CoC, reserve the right to review all individual agency requests for CSV and/or XML imports into Vermont's HMIS. In making a request, an agency must provide the CoC with documentation their vendor can meet the HUD standards for CSV and/or XML imports and confirmation the funding source allows imports. Once an agency's vendor has been approved, the CoC will evaluate importing as it relates to funding requirements and its potential impact on the data integrity of Vermont's HMIS. Allowing CSV and/or XML imports could impact data integrity and increase the likelihood of duplication of client files within the system. The data must meet minimum data completeness requirements set forth by HUD at not greater than 10% missing data fields with in each required Universal Data Element as defined in the most recent HMIS Data Standards Manual for each upload. Prior to an approved import, the agency requesting the import will incur all costs associated with the import, including, but not limited to: Bowman's cost of service and the HMIS Lead's cost of service. An estimate will be provided. However, the agency requesting the import will be responsible for any additional costs incurred directly related to the import process. All payments are non-refundable.

4.5 HMIS DATA PROTECTION

As the HMIS Lead Agency, it is the responsibility of ICA to maintain the HMIS, including protecting the data contained in HMIS. In the case where ICA is made aware through data contained in HMIS that Partner Agency program funds were used for an ineligible service, ICA will notify the Partner Agency about the misuse of funds. If the Partner Agency fails to rectify the misuse of funds in a timely fashion, ICA will notify the appropriate funding body.

5. Glossary

Agency Administrator – the individual responsible for HMIS use at each partner agency that has ten or more HMIS users.

Aggregated Public Data – data that is published and available publicly. This type of data does not identify clients listed in the HMIS.

Closed Data – information entered by one provider that is not visible to other providers using HMIS.

Confidential Data – contains personal identifying information.

ICA – the Institute for Community Alliances, which is the HMIS Lead Agency.

HMIS – Homeless Management Information System – an internet-based database that is used by homeless service organizations across Vermont to record and store client-level information about the numbers, characteristics and needs of homeless persons and those at risk of homelessness.

HMIS Advisory Board – the group of HMIS users who are responsible for approving and implementing the HMIS Policies and Procedures, and for working to make improvements to Vermont's HMIS.

HMIS License Fee – the annual fee paid by partner agencies to allow each HMIS user at their agency continued access to the database.

HMIS User Level – HMIS users are assigned a specific user level that limits the data the user is able to access in the database.

HMIS Vendor – the Vermont HMIS software vendor is Bowman Systems. The HMIS vendor designs the HMIS and provides ongoing support to the System Administrators.

Minimum Data Entry Standards – a minimum set of questions that must be completed for each client to provide data for use in aggregate analysis.

Open Data – does not contain personal identifying information.

Partner Agencies – the homeless service organizations that use HMIS.

System Administrators – staff in the Division of Housing who are responsible for overseeing HMIS users and use in Vermont. The System Administrators allow users HMIS access and provide training; ensure user compliance with HMIS policies and procedures; and make policy recommendations to the Steering Committee.

Shared Data – unrestricted information that has been entered by one provider and is visible to other providers using HMIS.

Unpublished Restricted Access Data – information scheduled, but not yet approved, for publication.

Victim Service Provider – a nonprofit agency with a primary mission to provide services to victims of domestic violence, dating violence, sexual assault, or stalking.

6. Appendices

6.1 USER MANUALS

The User Manuals for General Users provide the protocol for data entry workflow for Vermont HMIS users. The User Manuals include the data entry workflow requirements to document valid program entry and exit dates in the HMIS. Manuals are located on the ICA website: www.icalliances.org/vermont .

6.2 DATA DICTIONARY AND DATA MANUAL

The HMIS Data Standards Manual is intended to serve as a reference and provide basic guidance on HMIS data elements for CoCs, HMIS Lead Agencies, HMIS System Administrators, and users. The companion document to the HMIS Data Manual is the HMIS Data Dictionary.

The HMIS Data Dictionary is designed for HMIS vendors, HMIS Lead Agencies, and HMIS system administrators to understand all of the data elements required in an HMIS, data collection and function of each required element and the specific use of each element by the appropriate federal partner. The HMIS Data Dictionary should be the source for HMIS software programming.

HMIS systems must be able to collect all of the data elements defined in the HMIS Data Dictionary, support system logic identified in this document, and ensure that data collection and the visibility of data elements is appropriate to the project type and federal funding source for any given project.