Vermont Statewide

Homeless Management Information System

Policies and Procedures Version 4.0

VT HMIS Advisory Committee

in partnership with

Institute for Community Alliances

2024

**Contents**

[2.8 HMIS OPERATING POLICIES VIOLATION 5](#_Toc171327676)

**[1. Introduction](#_Toc171327678)** [6](#_Toc171327678)

[1.1 HMIS BENEFITS 6](#_Toc171327679)

**[2. Requirements for Participation](#_Toc171327680)** [7](#_Toc171327680)

[2.1 PARTNER AGENCY REQUIREMENTS 7](#_Toc171327681)

[2.2 RESPONSIBILITIES OF HMIS USERS 11](#_Toc171327682)

[2.3 User CONFLICT OF INTEREST 13](#_Toc171327683)

[2.4 USER TRAINING REQUIREMENTS 13](#_Toc171327684)

[2.5 HMIS ACCESS ROLES 15](#_Toc171327685)

[2.6 HMIS VENDOR REQUIREMENTS 16](#_Toc171327686)

[2.7 MINIMUM TECHNICAL STANDARDS 16](#_Toc171327687)

[2.8 HMIS LICENSE FEES 17](#_Toc171327688)

[2.9 HMIS OPERATING POLICIES VIOLATION 17](#_Toc171327689)

**[3.](#_Toc171327690)****[Privacy and Security](#_Toc171327690)** [19](#_Toc171327690)

[3.1 DATA CATEGORIZATION AND HANDLING 20](#_Toc171327691)

[3.2 DATA REPORTING PARAMETERS AND GUIDELINES 21](#_Toc171327692)

[3.3 RELEASE OF DATA FOR GRANT FUNDERS 21](#_Toc171327693)

[3.4 BASELINE PRIVACY POLICY 22](#_Toc171327694)

[3.5 USE OF A COMPARABLE DATABASE BY VICTIM SERVICE PROVIDERS 25](#_Toc171327695)

[3.6 DISASTER RECOVERY PLAN 26](#_Toc171327696)

[3.7 PARTNER AGENCY WORKPLACE REQUIREMENTS 27](#_Toc171327697)

[3.8 DATA SHARING EXTERNAL TO HMIS 27](#_Toc171327698)

[3.9 HMIS INTERNAL PRIVACY SETTINGS 28](#_Toc171327699)

[3.10 SECURITY PROCEDURE TRAINING FOR USERS 28](#_Toc171327700)

[3.11 VIOLATION OF SECURITY PROCEDURES 28](#_Toc171327701)

[3.12 PROCEDURE FOR REPORTING SECURITY INCIDENTS 28](#_Toc171327702)

[3.13 PROHIBITED HMIS ACTIVITIES 29](#_Toc171327703)

**[4. Data Requirements](#_Toc171327704)** [29](#_Toc171327704)

[4.1 MINIMUM DATA COLLECTION STANDARD 29](#_Toc171327705)

[4.2 PROVIDER NAMING CONVENTION 29](#_Toc171327706)

[4.3 DATA QUALITY PLAN 29](#_Toc171327707)

[4.4 DATA IMPORTS 30](#_Toc171327708)

[4.5 HMIS DATA PROTECTION 30](#_Toc171327709)

**[5. Glossary](#_Toc171327710)** [31](#_Toc171327710)

**[6. Appendices 1: Federal HMIS Requirements](#_Toc171327711)** [32](#_Toc171327711)

[6.1 USER MANUALS 32](#_Toc171327712)

[6.2 DATA DICTIONARY AND DATA MANUAL 32](#_Toc171327713)

[6.3 HMIS REGUALTIONS AND STANDARDS 33](#_Toc171327714)

**[7. Appendices 2: Data Quality Plan](#_Toc171327715)** [33](#_Toc171327715)

[7.1 GOALS OF THE DATA QUALITY PLAN 33](#_Toc171327716)

[7.2 DATA QUALITY PLAN AND RESPONSIBILITIES 33](#_Toc171327717)

[7.3 DATA COMPLETENESS 35](#_Toc171327718)

[7.4 DATA COMPLETENESS STANDARDS 35](#_Toc171327719)

[7.5 DATA CONSISTENCY 36](#_Toc171327720)

[7.6 DATA ACCURACY 37](#_Toc171327721)

[7.7 DATA ACCURACY STANDARD 37](#_Toc171327722)

[7.8 DATA TIMELINESS 38](#_Toc171327723)

[7.9 BED/UNIT UTILIZATIONS RATES 38](#_Toc171327724)

[7.10 MONITORING PLAN 38](#_Toc171327725)

[7.11 DATA QUALITY PLAN ENFORCEMENT 39](#_Toc171327726)

**Revision History**

|  |  |  |
| --- | --- | --- |
| **Section number**  | **Revision description**  | **Date approved** |
| N/A | Document page numbers added | BoS – 6.19.2018Chittenden – 8.2.2018 |
| N/A | Document updated to version 2.0  | BoS – 6.19.2018Chittenden – 8.2.2018 |
| 2.1 | Add obtain client release of information to user agreement. | BoS – 6.19.2018Chittenden – 8.2.2018 |
| 2.2 | Add agency responsibilities and timeline for notifying ICA of changes in users | BoS – 6.19.2018Chittenden – 8.2.2018 |
| 3.4 | Added clarification of written request for law enforcement requesting data | BoS – 6.19.2018Chittenden – 8.2.2018 |
| 3.4 | Remove historical data cannot be used to discriminate against clients. Add historical data cannot be used for eligibility purposes. | BoS – 6.19.2018Chittenden – 8.2.2018 |
| 3.8 | Delete “if possible” change locate to reached. | BoS – 6.19.2018Chittenden – 8.2.2018  |
| 3.10 | Update vendor name | BoS – 6.19.2018Chittenden – 8.2.2018 |
| 5 | Add additional glossary terms | BoS – 6.19.2018Chittenden – 8.2.2018 |
|  | Updated ServicePoint with Bitfocus Community Service (ServicePoint) throughout | BoS – 4.16.2019Chittenden – .6.6.2019 |
| 2.1 | Added timeframe for agencies to notify lead agency of staffing changes | BoS – 4.16.2019Chittenden – .6.6.2019 |
| 2.1 | Specified requirements for creating and maintaining strong passwords | BoS – 4.16.2019Chittenden – .6.6.2019 |
| 2.4 | Defined role of Executive Director as user type in HMIS | BoS – 4.16.2019Chittenden – .6.6.2019 |
| 2.7 | Modified Advisory Committee will be made aware of HMIS license costs not approve costs | BoS – 4.16.2019Chittenden – 6.6.2019 |
| 2.8 | Removed Advisory Committee vote to revoke user licenses for chronic misuse.  | BoS – 4.16.2019Chittenden – 6.6.2019 |
| 3.1  | Updated for consistent use of terms used in document, reorganized for better clarity | BoS – 4.16.2019Chittenden – 6.6.2019 |
| 3.4 | Requirement to disclose PII to law enforcement source cited, additional language to strengthen this as optional of providers | BoS – 4.16.2019Chittenden – 6.6.2019 |
| 4.3 | Data quality plan improvement steps stated and removal of punitive language | BoS – 4.16.2019Chittenden – 6.6.2019 |
| Glossary | Removed “Division of Housing” from System Administrator | BoS – 4.16.2019Chittenden – 6.6.2019 |
| Multiple Sections | Replaces WellSky Community Services with new vendor name; Bitfocus Clarity | BoS 2022Chittenden 2022 |
| 2.4 | Updated User Roles to reflect the new Access Roles from Bitfocus Clarity | BoS 2022Chittenden 2022 |
| 3.1: Shared Data | Removed ‘not’ | BoS 2022Chittenden 2022 |
| 3.4: Limits on Partner Agency Use of HMIS Client Information  | Removed ‘regionally’Added: Data is shared with agencies that are listed in the VT Agencies Using HMIS document. This list is subject to change. | BoS 2022Chittenden 2022 |
| Multiple sections | Removed ‘Agency Administrator’ and replaced with’ Designated HMIS Agency Contact(s)’ | BoS 2022Chittenden 2022 |
| N/A | Document updated to version 3.0 | BoS 2022Chittenden 2022 |
| 2.8 HMIS OPERATING POLICIES VIOLATION | Added Agency violations and updated the repercussions.  | BoS 2022Chittenden 2022 |
| 2.1 | Added Two Factor Authentication Policy |  |
| 2.1 | Update Consumer Consent for Sharing Data Forms  |  |
| 2.2 | Addition to responsibility of Agency/Designated HMIS Agency Contact and UserExplanation of extended leave |  |
| 2.3 | Verbiage updates |  |
| 2.4 | Verbiage updates |  |
| 2.5 |  Verbiage updates |  |
| 2.6 | Updates to reflect for new database needs |  |
| 2.8 | Verbiage updates |  |
| 3 | Added multiple sections |  |
| 4.5 | Added verbiage on us of AI and HMIS in public presentations |  |
| 5 | Updated Glossary: BHS definition |  |
| 6 | Updated name of section |  |
| 7 | Added completely new section |  |
| Multiple | Replace ‘client’ with ‘consumer’ to ensure consistence throughout document |  |

**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 Bitfocus Clarity, 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. Bitfocus, hereinafter called ‘Vendor’, administers the central server and HMIS software, and ICA administers user and agency licensing, training and compliance. Use of HMIS is mandated by the U.S. Department of Housing and Urban Development (HUD) and by federal partners including the U.S. Department of Health and Human Services and the U.S. Department of Veterans Affairs. The State of Vermont, local government entities and some private funders also require Partner Agency participation in HMIS.[[1]](#footnote-2)

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 an Advisory Committee made up of a geographically diverse group of HMIS Users, homeless service providers, policy makers, funders and CoC Leadership, who 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 Designated HMIS Agency Contacts and end users.[[2]](#footnote-3)

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 secure 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.
* Allows for data informed allocation of staff, time, financial and other 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 PARTNER AGENCY REQUIREMENTS

The homeless service organizations that use HMIS, hereinafter called ‘Partner Agency’, must adhere to the following requirements.

Participation Agreement Documents

Partner Agencies must complete the following documents:

1. **Partnership Agreements** must be signed by each Partner Agency’s Executive Director or authorized representative. The Institute for Community Alliances will retain the original document. The Partnership Agreement states the Partner Agency’s commitment to adhere to the policies and procedures for effective use of HMIS.
2. **Vermont HMIS User Agreements** list userpolicies and responsibilities and are electronically signed by each authorized HMIS user at Partner Agency. An electronic or hard copy of the original document must be kept by the originating Partner Agency.
3. **Coordinated Services Agreements** allow the specifically named HMIS user to enter client data as, or on behalf of, another specifically named Partner Agency and/or to report on behalf of the specifically named Partner Agency. The signed agreement will be maintained by the HMIS Lead Agency, the Institute for Community Alliances (ICA).

User Access to the System

The HMIS System Administrator will determine user access for users and assign users to the appropriate agency. The HMIS System Administrator will generate usernames and passwords within the administrative function of the software.

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

It is the responsibility of the Partner Agency Executive Director or designee, such as the Designated HMIS Agency Contact, to notify the HMIS Lead Agency within 24 hours when a HMIS user in their agency no longer needs access to HMIS.

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, and record volunteer hours with the agency. It is strongly recommended that all users, including official volunteers, undergo a criminal background check. 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 Vermont HMIS User Agreement. Users must disclose any potential conflict of interest to their System 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: Temporary passwords are issued when a user is created. The System Administrator will communicate the temporary 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 long and contain a minimum of one upper and one lowercase letter, numeric character, and special character. Passwords should not be easily guessed, found in a dictionary, or if you are aware it has been previously compromised. 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 people. Users are not allowed to store passwords on a personal computer for easier login access.
* Expiration: Passwords expire every 90 days. Users may not use the same password consecutively or reuse previous passwords.
* Unsuccessful login: If a user unsuccessfully attempts to login 4 times, their User ID will be “locked out,” and access permission will be revoked rendering the user unable to gain access until their password is reset. Users can utilize the Password Reset function to regain access to the HMIS.

Two-Factor Authentication (2FA)

All HMIS system administrators and end users must have a unique email address associated with their user account. Most partner agencies have agency issued email addresses; this will be used for those agencies. In the case where agencies do not have agency issued email addresses, the HMIS lead agency may consult with or encourage the agency to use a free service, like Google Workspace for non-profits.

Authentication is directly related to the unique user ID, computer, and web browser.

In addition to a unique email address, HMIS users will be assigned a unique user ID and be required to create a strong password every 90 days.

· The vendor requires the following for password strength:

o Must be 8 characters or longer and contain all four of the following:

* English uppercase character (A through Z)
* English lowercase character (a through z)
* Numerals (0 through 9)
* Non-alphabetic characters (such as: !, $, #, % , etc.)

o \* Your password cannot contain your username, cannot be a take on the word 'clarity', and cannot be the same one as before.

All HMIS users will be required to use Two-Factor Authentication to access the HMIS. The HMIS is configured to accept email authentication tokens or an authenticator application token. The HMIS lead agency strongly recommends using an authenticator application as it is the current best practice.

· Email authentication is directly linked to the unique email address associated with the user’s account.

· Authenticator applications may be used on work or personal devices. Please verify and comply with your agency’s technology policies regarding the use of personal devices.

With two-factor authentication, each HMIS user will have the ability to mark their designated daily work issued computer / tablet as a trusted device. If marked as a trusted device, authentication will be required every 90 days.

· What is a trusted device?

o Non-public work issued computer or tablet

· What is not a trusted device?

o Public computer / tablet (library or day station shared computer)

|  |  |  |
| --- | --- | --- |
| **Device** | **HMIS Usage** | **Trusted Device** |
| Work Issued | Yes | Yes |
| Personal (e.g. home computer connected to secure wifi with password and router with password) | Yes | No |
| Public (e.g. library computer) | No | No |

 **Please note:** Trusted devices should never be used on a public, open, free, or unsecured internet connection. A trusted device may use a work issued secure Wi-Fi hotspot in a public location.

Entering Data

Partner 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 immediately to the HMIS Lead Agency.

Client Consent for Sharing Data Forms

Agencies are required to ensure clients know what data is being collected about them and that the data will be shared among all participating agencies within the HMIS.

1. The HMIS Consumer Privacy Notice must be posted in a location visible to clients when collecting client data.
	1. This privacy notice informs consumers that their data will be entered into the HUD CoC HMIS. Consumers do not provide permission to have data entered, only to share the data.
2. Agency staff must be able to provide a copy of the HMIS Baseline Privacy Statement upon client request.[[3]](#footnote-4)
3. Clients may elect to share or not share their information with HMIS Participating Agencies and CoC Data Partners.
4. Agencies are required to ensure clients are given the opportunity to make choices about their personal and program related information that is shared in HMIS.
5. Agencies are required to use the Client Consent form on the ICA website.
	1. The form requires clients to authorize the electronic sharing of their personal information with other Partner Agencies that participate in HMIS when data sharing is appropriate for client service
	2. The form allows the client to exercise their right to opt-out of data sharing in the cases where they have discretion.
6. Agencies must allow clients the opportunity to review and correct information in their own client record to make sure that information is accurate.

Data Protocols

Agencies participating in the HMIS must meet the minimum data entry requirements established under the most recent HMIS Data Standards.[[4]](#footnote-5) Partner Agencies may collect information for data elements in addition to the minimally required data elements established by the HMIS Advisory Committee in accordance with HUD.

Partner Agencies must maintain consistency with data collection and entry within each program.[[5]](#footnote-6).

Agency Relationship with the HMIS Vendor

Partner Agencies are prohibited from directly contacting the HMIS Vendor to request custom database work. Any such request must be made through the HMIS Lead Agency.

2.2 RESPONSIBILITIES OF HMIS USERS

Designated Agency Security Officer

Each Partner Agency must designate a Security Officer. The Security Officer must be a current HMIS user and may also be the Designated Agency HMIS Contact. The Security Officer is responsible for maintaining the security of the HMIS for their agency. They must verify compliance with applicable security standards, monitor HMIS access by users at their agency, and ensure the participating agency obtains a unique user license for each user at the agency.

Designated Agency HMIS Contact

Each Partner Agency must designate an Agency HMIS Contact. This person serves as the primary agency point of contact for all matters concerning HMIS.

The Designated Agency Security Officer and Designated Agency HMIS Contact may be the same person at the agency.

Designated HMIS Agency Contacts Responsibilities

User Accountability at Agency

* Ensure HMIS access is granted only to staff members that have received training by the System Administrators, have completed the Vermont User Agreement and are authorized to use HMIS.
* Ensure agency users receive required on-going or annual HMIS training. Ensure agency users review the Vermont HMIS Policies and Procedures, the Agency Partnership Agreement and any agency policies which impact the security and integrity of client information.
* Notify all users at their agency of interruptions in service.

Program Information

* 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 in HMIS.
* Maintain the required Universal Data Elements and program specific data elements for each program in accordance with the most recently released HMIS Data Standards and maintain data elements required by the HMIS Advisory Committee and/or the CoC in which the program operates.
* Identify the assessment and reporting requirements for each program.

Agency Communication with ICA

* Provide a single point of communication between users and HMIS staff at the Institute for Community Alliances.
* Provide updated agency and program information to ICA and work with System Administrators to properly set up each program in the HMIS.
* Provide the System Administrator with the reason User needs to enter data, so the appropriate access role is determined. In all cases, the System Administrator will generate usernames and temporary passwords within the administrative function of the software.
* Notify the System Administrator within 24 hours when a HMIS user in their agency is going to be on extended leave, vacation or leaving their position.

General HMIS Users

Users are considered general HMIS users if they enter data into HMIS for a Partner Agency that has housing projects listed on their CoC’s Housing Inventory Count, or for a Partner Agency that is required by the entity that funds their homeless service or housing project to enter data into HMIS

HMIS User Responsibilities

1. Take appropriate measures to prevent unauthorized data disclosure.
2. Not show the HMIS to anyone that is not currently licensed in the HMIS. I will reach out to the HMIS System Administrator to notify them of the request.
3. Report any security violations to the HMIS System Administrator.
4. Comply with relevant policies and procedures.
5. Input required data fields in a current and timely manner. (Best practice is within 5 days with up to 30 days grace period.)
6. 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.
7. Inform clients about the agency’s use of HMIS and secure all required releases of information for sharing client data
8. Take responsibility for any actions undertaken with one’s username and password.
9. Complete required training.
10. Read the Vermont HMIS News email newsletter.
11. Notify the HMIS System Administrator if user is going to be out on extended leave, vacation or leaving their position.
12. Intentionally falsifying data on behalf of a client for the purposes of affecting program eligibility is prohibited
13. Agree to not access HMIS on an open, public, or unsecured network or public device.

NOTE: If a user does not log in for 90 days or more, their user account will automatically be made inactive. This will prompt the HMIS System Administrator to require the user to take the Refresher Training.

2.3 User CONFLICT OF INTEREST

Users who have their own client files in HMIS are prohibited from viewing, entering, or editing information in their own file. All users are prohibited from viewing, 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 Designated Agency HMIS Contact. The agency must inform ICA of the conflict of interest and state the agency’s policy to address it. The System Administrator may run the User Activity Report to determine if there has been a violation of the conflict-of-interest agreement.

2.4 USER TRAINING REQUIREMENTS

Agency Responsibilities for User Training

It is the responsibility of the Partner Agency to inform and ensure each user at their agency, completes the training and data entry requirements.

Full participation and attention to all training courses attended is expected.

New HMIS User Training Requirements

Any potential HMIS user is required to attend the new user training with the HMIS Lead Agency, prior to receiving access to the system. If the HMIS Lead Agency determines that data entered by a current HMIS User does not meet minimum data quality standards, users may be required to repeat this training.

Once a new user begins the training series, they have 30 days to complete the training series and any required assignments. If the user fails to complete all requirements within 30 days, the user will need to begin the training series again. HMIS System Administrator staff may determine that a new user failed to grasp the necessary data entry concepts and may use their discretion to require them to repeat new user training. If a new user fails to successfully complete the training requirements for data entry after repeated attempts, HMIS System Administrator 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 HMIS user license and had a license for the Vermont HMIS in the past, the user will be required to re-take the training series, with few exceptions. The HMIS Lead Agency has sole discretion to waive the requirement to attend new user training. The HMIS Lead Agency 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 the training courses 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.

New User Training Requirements for Previous Users

If a user requesting a new user license previously had a license in the system, the user will still be required to retake the New User 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.

Annual HMIS Security and Privacy Training for All Users

All users are required to attend the designated Annual HMIS Security and Privacy Training to retain their user license. Information for when this training is posted each year will be provided through the HMIS newsletter.

Annual Training for All Users

Each user is responsible for reviewing the training documents and videos related to their specific project and funding. Links to these trainings are provided through the [ICA Knowledge Base.](https://icanewengland.helpscoutdocs.com/collection/1-vermont-hmis-users)

In addition, users may be required to take a designated Annual Training required by ICA.

If ICA designates an Annual Training requirement, agencies and users can expect to be notified of this training through the HMIS newsletter and be given the duration of the calendar year to complete the required training. All users regardless of status in the system may be required to take the designated Annual Trainings.

If ICA staff determine at any point that HMIS data entry concepts are not grasped based on the quality of the user’s work in the system, ICA staff may use their discretion to require users to repeat new user training or attend other additional trainings.

HMIS Report Platform Training

If users would like to gain access to the HMIS reporting platform, Data Analysis (Looker) License, they are required to attend at least one Data Analysis training annually, in addition to the required general HMIS trainings.

All users with licenses for the reporting platform embedded in HMIS, along with the Designated Agency HMIS Contact are required to review the training requirements for the reports their agency needs to utilize, in addition to the required general user HMIS trainings. Links to these trainings are provided through the [ICA Knowledge Base.](https://icanewengland.helpscoutdocs.com/collection/71-new-hampshire-hmis-users)

Coordinated Entry HMIS Training

Coordinated Entry Training is considered part of the New User Training. Each HUD CoC will establish their requirements for training related to Coordinated Entry in coordination with ICA. ICA will provide the HMIS specific workflow and report trainings as required by the HUD CoC. Agencies and users are responsible for checking with their HUD CoC leadership for these requirements.

User License Suspension – Training Requirements

The HMIS Lead Agency will suspend user licenses from users who do not complete their annual training requirements within 60 days of the announced training start date. To reactivate the license, the user must complete their training requirements.

NOTE: The Executive Director and direct manager must review the relevant governance documents related to the agency responsibilities related to HMIS.

2.5 HMIS ACCESS ROLES

Access Roles designate what data and capabilities a HMIS User can access in the HMIS.
Find more details here: <https://help.bitfocus.com/rights-glossary-for-access-roles>

Access Roles are created with the following:

* Seat Type
	+ Admin: access to all *Access Role* rights
	+ Manager: access to all *Access Role* rights except for*Any Agency Sensitive Data*and *Data Import*
	+ Enterprise: same access level as *Manager* except for *Manage Agency*, *Data Analysis, Data Analysis Save,*and *Aggregate Data Analysis*
* Access Role Rights
	+ System Administrator Rights
		- ICA HMIS Staff will still have these rights.
	+ Access Rights: Access rights provide staff members **access** to specific components of the client record, agency and program management, and Clarity Human Services functionality. If the right is toggled off for an access role, staff members with that access role will not be able to access the corresponding functionality.
	+ Create Rights: **Create Rights** give staff members the ability to **create**and**record** specific types of data in client records.
	+ Edit Rights: **Edit** provide staff members the ability to **edit** and**delete** existing data in client records, either at the agency level or across all agencies (subject to[sharing settings](https://help.bitfocus.com/introduction-to-sharing-client-data)).
	+ Delete Rights: **Delete Rights** provide staff members the ability to **delete** existing data in client records, either at the agency level or across all agencies (subject to[sharing settings](https://help.bitfocus.com/introduction-to-sharing-client-data)).

2.6 HMIS VENDOR REQUIREMENTS

Physical Security

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

Firewall Protection

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

Vendor will assist the HMIS Lead Agency to resolve software problems, make necessary modifications for special programming, and will explain system functionality to the HMIS Lead Agency.

Technical Performance

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 10
* The most recent version of Google Chrome, Microsoft Edge, Apple Safari or Mozilla 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

Additional Recommendations

Memory

* + Windows 10: 4 Gig 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

Partner Agencies may purchase licenses at any time. The amount of a user license may change depending on the operating costs of the Vermont HMIS. The amount charged for user licenses is dependent on the operating costs of the Vermont HMIS. The HMIS Advisory Committee will be notified of changes in cost and given the opportunity to ask questions regarding the impact of such change.

Billing for licenses will occur once annually, covering July - June. The annual fee 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 the HMIS Lead Agency receives the payment.

HMIS Reporting Platform Licenses

The reporting platform 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. This cost is subject to annual review.

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 HMIS 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 to be considered second or third violations. Violations do not expire; no regard is given to the duration of time that occurs between successive violations.

As the contract holder with the HMIS Vendor, ICA is the only entity that will have contact with the HMIS Vendor. If a User or Partner Agency has any questions, concerns, suggestions, etc., they should contact their HMIS System Administrator. This will lessen confusion and the occurrence of misleading information. If you need more information, contact your HMIS System Administrator; vtmis@icalliances.org

Examples of User and Partner Agency violations include in the below Repercussions section but are not limited to:

* Interactions with the HMIS Vendor
	+ Emailing staff at HIS Vendor
	+ Requesting and/or scheduling a meeting with HMIS Vendor staff
	+ Attending HMIS Vendor trainings
	+ Participating in virtual platforms that are specific to the HMIS Vendor
		- Such as their Slack channel(s)
* Sharing username and password
* Sharing client level data with agencies or persons that the client did not give permission to share.
* Using client data to discriminate against a client or refuse service
* Enter data in HMIS that makes a client pull as chronically homeless when they are not.

Repercussions

* + First Violation – the user and/or Partner Agency will be notified of the violation in writing by the HMIS Lead Agency. If a user violation, the user’s license will be suspended until the user participates in a live Security and Privacy training. If there is an agency violation, all user licenses will be suspended until all users participate in a live Security and Privacy training. The HMIS Lead Agency will notify the HMIS Advisory Committee of the violation during the next scheduled Advisory Committee meeting following the violation.
	+ Second Violation – the user and/or Partner Agency will be notified of the violation in writing by the HMIS Lead Agency. If there is a user violation, the user’s license will be suspended for 30 days. The user will also be required to participate in a live Security and Privacy training. 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 user has participated in a live Security and Privacy training. If an agency violation, all user licenses will be suspended for 30 days. All users will also be required to participate in a live Security and Privacy training. 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 all users have participated in a live Security and Privacy training. The HMIS Lead Agency will notify the HMIS Advisory Committee of the violation during the next scheduled Advisory Committee meeting following the violation.
	+ Third Violation – The HMIS Lead Agency will notify the user and/or Partner Agency of the violation in writing. The HMIS Lead Agency will notify the HMIS Advisory Committee of the violation. The HMIS System Administrator and HMIS Advisory Committee will determine what the repercussions for the user or agency will be. If the user has an additional violation after their third violation, their license will be terminated, and the Advisory Committee will be notified. If an agency has an additional violation after their third violation, a fee will be incurred by that agency. This fee will be determined by the HMIS System Administrator and the HMIS Advisory Committee. User licenses will be suspended until the fee is paid in full. A minimum fee of $500 would be incurred by the agency with the potential for this fee to significantly rise depending on System Administration time and if Vendor involvement is needed.

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 or Security Breach

It is the responsibility of the Designated HMIS Agency Contact or general user at Partner Agencies that do not have a Designated HMIS Agency Contact, 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 by the HMIS Lead Agency if the individual wishes to remain anonymous.

In the event that the suspicion of violation of use is about an employee of the HMIS Lead Agency, the Designated HMIS Agency Contacts or reporting user should contact both the affected HUD Continuum of Care leadership as well as the direct HMIS Lead Agency managing director.

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 HMIS Lead Agency 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 the HMIS Lead Agency to collaboratively update the applicable policies for the Partner Agency to accurately reflect the additional protections.

3.1 DATA CATEGORIZATION AND HANDLING

All HMIS data will be handled according to the following major classifications: Shared Data or Not Shared Data. The HMIS Lead Agency 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 partner agency and is visible to other partner agencies using HMIS. Vermont’s HMIS is designed as a *share*d system that defaults to sharing data.

Not Shared Data

Data that is *not shared* is information entered by one provider that is not visible to other providers using HMIS. Data must not be shared by programs that provide services to unaccompanied minors, or legal services. Individual client enrollments that have been shared can be changed to *not shared* at the client’s request.

Confidential Data at the Partner Agency Level

Confidential Data contains personal identifying information. Each Partner 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 Partner 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.

Open Data

Data that does not contain personal identifying information should be handled discreetly, unless it is further classified as Public Data. This type of data must be stored securely and not left accessible by unauthorized personnel. Open data may be shared via internet or first-class mail until the data is considered Public Data at which time specific classification will dictate any ongoing sharing rules.

Public Data

All Public Data falls into one of two classifications: *Aggregated Public Data* or *Unpublished Restricted Access Data.* Each classification has its own procedures that must be observed.

Aggregated Public Data

This data can be released to the public following the principles outlined in Section 3.2 Reporting Parameters and Guidelines because there is no identifying information that could lead back to a specific client or household served.

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. This type of data requires the following procedures to be observed and followed:

* 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: Always requires encryption. 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

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 Partner 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 Partner 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.
* The HMIS Lead Agency reserves the right to deny any request for aggregated data. Final decisions will be made by the HMIS Director.

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 the HMIS Lead Agency when there is a voluntary written agreement in place between the funding entity and the Partner Agency or program. Funding for any Partner 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 Partner 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 of their personal information as described in this notice when they seek assistance from a Partner Agency using HMIS and provide the Partner Agency with their personal information. Explicit permission is required to 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 a Partner 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.
2. To carry out administrative functions such as legal audits, personnel, oversight, and management functions.
3. For research and statistical purposes. Data released for research and statistical purposes will not include Personally Identifying Information.
4. For academic research conducted by an individual or institution that has a formal relationship with the HMIS Lead Agency. 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 HMIS Agency Contacts or Executive Director. The written research agreement must:
* Establish the rules and limitations for processing personal information and providing security for personal information during 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.
1. When required by law Personal information will be released to the extent that disclosure complies with the requirements of the law.
2. 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 HMIS Lead Agency 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 agency or organization may, but is not required to release client information providing the request meets the following requirements, according to the Federal Register /vol.69 No. 146:
1. Be signed by a supervisory official of the law enforcement agency seeking the personal information.
2. State how the information is relevant and material to a legitimate law enforcement investigation.
3. Identify the personal information sought.
4. Be specific and limited in scope to the purpose for which the information is sought.
5. Be approved for release by the HMIS Lead Agency's legal counsel after a review period of seven to fourteen days and,
6. Have written consent for client data release from the respective governing HUD recognized Continuum of Care.
* If it is believed that the personal information constitutes evidence of criminal conduct that occurred at the Partner 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 head 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.
1. 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.
2. 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.
1. 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.
1. To comply with government reporting obligations for homeless management information systems and for oversight of compliance with homeless management information system requirements.

Inspection and Correction of Personal Information

Clients may inspect and receive a copy of their personal information maintained in HMIS. The Partner Agency where the client receives services will offer to explain any information that a client may not understand. The Partner Agency will provide the requested personal information to the client within no more than 60 days or as required by agency guidelines, whichever is soonest.

If the information listed in HMIS is believed to be inaccurate or incomplete, a client may submit a verbal or written request to have their 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
* The life or physical safety of any individual would be reasonably endangered by disclosure of the personal information, or
* If requests are made in a repeated and/or harassing manner.

If a request for inspection access or personal information correction is denied, the Partner Agency where the client receives services will explain the reason for the denial. The Partner Agency will provide the reason for denial to the client within no more than 60 days or as required by agency guidelines, whichever is soonest. The client’s request and the reason for the denial will be included in the client’s record.

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. The HMIS Lead Agency will check with Partner 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 a shared data system. This system allows Partner Agencies to share client information to coordinate services for clients. However, Partner Agencies may not limit client service or refuse to provide services based on historical data contained in HMIS enrollment dates (as verified by a Partner Agency) may be used towards program eligibility documentation as allowable by HUD, but data within the enrollment may not as it is client self-report. Data is shared with agencies that are listed in the VT Agencies Using HMIS document. This list is subject to change: <https://icanewengland.helpscoutdocs.com/article/282-vermont-hmis-governance>

Youth providers serving clients under the age of 18 must maintain Not Shared 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, unless they are emancipated or otherwise have the legal authority to do so.

Complaints and Accountability

Questions or complaints about the privacy and security policies and practices may be submitted to the Partner Agency where the client receives services. Complaints specific to HMIS should be submitted to the Designated HMIS Agency Contact and Program Director. If no resolution can be found, the complaint will be forwarded to the System Administrators, and the Partner Agency’s Executive Director. If there is no resolution, the Vermont HMIS Advisory Committee will oversee final arbitration. All other complaints will follow the Partner 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 DISASTER RECOVERY PLAN

Bitfocus Disaster Recovery Plan

Vermont’s HMIS is covered under Bitfocus Disaster Recovery Plan. Due to the nature of technology, unforeseen service outages may occur. The disaster recovery plan is meant to minimize any effects of service outages and to enable Bitfocus to either maintain, or quickly resume, mission-critical functions. A copy of this plan is available for review by submitting a request to the VT HMIS Help Desk; vthmis@icalliances.org.

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. 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 no more 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. Bitfocus support staff help 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 (ICA), as HMIS Lead Agency, operates a regional approach to administering the Vermont HMIS. 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.

3.7 PARTNER AGENCY WORKPLACE REQUIREMENTS

1. The agency must apply system security provisions to all the systems where HMIS data is accessed including networks, desktops, laptops, smart devices, mainframes, and servers.
2. When HMIS is accessed in public areas the agency must ensure that the workstation is always supervised by authorized HMIS users. Screens displaying the HMIS may not be visible by unauthorized individuals.
3. Devices and data must be secured when workstations are not in use and staff are not present. Workstations must automatically turn on a password protected screen saver when the workstation is temporarily not in use. Staff are required to log off the HMIS when not at the workstation.
4. The agency must ensure all privacy and security requirements are always adhered to in remote work locations.

3.8 DATA SHARING EXTERNAL TO HMIS

Disclosure of client personal information to third parties requires a formal written agreement, authorized by the HMIS Advisory Committee. If an agreement is compatible with a prior authorization that is still in effect, ICA may enter into an agreement that does not require secondary authorization after notifying the HMIS Advisory Committee.

Third parties seeking client personal information from the Vermont HMIS will be required to complete a standard application designed to gather information regarding the information requested, the rationale for disclosure of the data (i.e., the benefits to persons experiencing/at risk of homelessness), and the scope of the project (i.e., one-time, or ongoing). The application will be subject to legal review, after which the HMIS Advisory Committee will vote on whether to enter into the proposed agreement.

Third parties with which ICA has a written data sharing agreement for the purpose of service delivery coordination and improvement are referred as “network partners.” As with HMIS-participating agencies, clients will have the opportunity to opt-out of sharing their data with network partners through the HMIS Release of Information. An up-to-date list of network partners will be posted on the ICA Vermont website.

Any external sharing of client personal identifying information will utilize secure transmission methods that meet industry standards, such as Secure File Transfer Protocol (SFTP), or through the use of an Application Programming Interface (API).

3.9 HMIS INTERNAL PRIVACY SETTINGS

The Vermont HMIS is a shared system. The default privacy settings for all client data entered by Partner Agencies are shared. Shared data is unrestricted information that has been entered by one provider and is visible to other providers using HMIS.

All Partner Agencies have the option to change their HMIS project settings to not share their client data with other Partner Agencies. Information entered by one Partner Agency that is not shared will not be visible to other Partner Agencies using HMIS. Projects that provide legal services, or serve individuals with HIV/AIDS, unaccompanied minors, or victims of domestic violence (when the participating agency is not a victim service provider), must have their client data visibility set to not shared. Projects that provide legal services may enter clients as “unnamed.” Through the HMIS Release of Information, clients may request that their individual client record is not shared going forward. Client records that were shared and contain data entered by multiple agencies cannot retroactively be closed. Individual components of the client record may be closed but the entire client record cannot be closed.

3.10 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.

3.11 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 Committee.

3.12 PROCEDURE FOR REPORTING SECURITY INCIDENTS

Users and Designated HMIS Agency Contacts 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.

3.13 PROHIBITED HMIS ACTIVITIES

The use of any Artificial Intelligence (AI) in the HMIS is prohibited.

The use of HMIS screen sharing, screenshots or other visuals that are of the inside of the HMIS during public presentations is prohibited by non- ICA staff. If agencies would like to conduct internal meetings or trainings for their HMIS users, they will need to contact ICA to review the contents of what they will be reviewing.

**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 Designated HMIS Agency Contact must identify the assessments and requirements for each program. The HMIS Lead Agency will consult with the Designated HMIS Agency Contact 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 Designated HMIS Agency Contacts and posted on the Institute for Community Alliances' Vermont HMIS webpage. Designated HMIS Agency Contacts 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 Lead Agency staff will monitor data collection of the HMIS Universal Data Elements and required program specific data elements monthly and hold Partner Agencies accountable for not entering required data.

The HMIS Lead Agency will submit a report to each CoC annually that identifies the degree to which all Partner 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 work with ICA to create a corrective action plan to address the data needs of the partner agency.

4.4 DATA 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, a Partner Agency must provide the CoC with documentation that their vendor can meet the HUD standards for CSV and/or XML imports and confirmation the funding source allows imports.  Once a Partner 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 within each required Universal Data Element as defined in the most recent HMIS Data Standards Manual for each upload. Prior to an approved import, the Partner Agency requesting the import will incur all costs associated with the import, including, but not limited to: Bitfocus’ cost of service and the HMIS Lead Agency’s cost of service.  An estimate will be provided. However, the Partner 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**

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

**Client-** Person or persons receiving services from an agency using the VT HMIS system for data collection.

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

**Confidential Data** – Contains personal identifying information.

**Designated HMIS Agency Contact -** This person serves as the primary agency point of contact for all matters concerning HMIS.

**Extended Leave / Vacation –** An extended leave would be 30 or more days.

**General HMIS User -** Users are considered general HMIS Users if they enter data into HMIS for a Partner Agency that has housing projects listed on their CoC’s Housing Inventory Count, or for a Partner Agency that is required by the entity that funds their homeless service or housing project to enter data into HMIS.

**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 Committee** – The group of HMIS users and other community stakeholders who are responsible for approving and implementing the HMIS Policies and Procedures, and for working to make improvements to Vermont’s HMIS.

**HMIS User Group -** Group forum for all HMIS Users to discuss the functionality of the HMIS, identify strengths and weakness and create the opportunity for HMIS Users to learn from each other.

**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 –** End user, employed by a local agency required to enter data. HMIS users in order to have access to the VT HMIS must pass and adhere to the minimum training and security standards.

**HMIS Access Role** – HMIS users are assigned a specific access role that limits the data and features the user is able to access in the database.

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

**ICA** – The Institute for Community Alliances, which is the HMIS Lead Agency and System Administrator.

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

**Official Volunteer -** A recognized and consistent unpaid member of a user agency. They may or may not have access to the VT HMIS. To have access they must pass and adhere to the minimum training and security standards.

**Open Data** – Does not contain personal identifying information.

**Partner Agencies** – The homeless service organizations that use HMIS.

**Security Officer -** Each Partner Agency must designate a Security Officer. The Security Officer must be a current HMIS user and may also be the Designated HMIS Agency Contact. The Security Officer is responsible for ensuring compliance with applicable security standards, monitoring HMIS access by users at their agency, and maintaining the security of the HMIS for their agency.

**System Administrators** –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 1: Federal HMIS Requirements**

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: <https://icanewengland.helpscoutdocs.com/> .

6.2 DATA DICTIONARY AND DATA MANUAL

The [HMIS Data Standards Manual](https://www.hudexchange.info/resource/3824/hmis-data-dictionary/) 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](https://www.hudexchange.info/resource/3824/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.

6.3 HMIS REGUALTIONS AND STANDARDS

The [2004 Data and Technical Standards Notice](https://files.hudexchange.info/resources/documents/2004HUDDataandTechnicalStandards.pdf) specifies the privacy and security standards for HMIS. The standards seek to protect the confidentiality of personal information while allowing for reasonable, responsible, and limited uses and disclosures of data.

**7. Appendices 2: Data Quality Plan**

Data quality is vitally important to the success of the HMIS and the programs that use this database. The Federal Partners and other funders monitor the quality of the HMIS data through the Annual Homelessness Assessment Report, System Performance Measures, the CoC Program Competition, and a variety of other program reports. If the quality of the data is poor, funders may refuse to grant funding or reduce future funding. These funding cuts could negatively affect program(s) throughout the State of Vermont. As it is imperative that the data is correct, HMIS participating providers and ICA staff will work diligently on adhering to the HMIS Data Standards to ensure all reports are complete, consistent, accurate, and timely.

7.1 GOALS OF THE DATA QUALITY PLAN

In coordination with the Vermont HMIS Advisory Committee, a data quality plan was established. The goals of this plan are to:

* Help ensure the availability of timely and accurate data for use in helping to end homelessness.
* Identify problems early and increase the usability of data.
* Prepare data for federal, state, and local reporting processes.
* Support the efforts of the HEARTH Act implementation, including Coordinated Entry.

Agencies and program providers will benefit from participating in the data quality plan for the following reasons:

* Fewer corrections will be required before reports are due because data will be corrected regularly.
* Access to more up-to-date information to inform program decisions, monitor client progress, and inform stakeholders about programs will be available.
* Accurate data will make performance measurement and program improvement possible.

7.2 DATA QUALITY PLAN AND RESPONSIBILITIES

Vermont HMIS Advisory Committee Overview

The Vermont HMIS Advisory Committee is made up of a group of HMIS users from all CoCs. The group meets on a bi-monthly basis and is responsible for approving and implementing the HMIS Policies and Procedures, and for working to make improvements to Vermont HMIS. For more details please refer to the VT HMIS Advisory Committee Governance Charter.

Vermont HMIS Advisory Committee Role

* Have an ongoing relationship with the HMIS users from across the CoCs to identify training needs.
* Develop the HMIS Policies and Procedures, including a Data Quality and Security Plan, which are updated annually.
* Meet at least annually to discuss changes to HMIS Policies and Procedures and updates in the system related to HMIS Data Quality.

Funder Role

* Create a framework of performance expectations that will enable the funder to rank and rate projects and target funding based on need.
* Monitor the established baseline standards for participation and data collection as set forth by the HMIS Data Standards.
* Work with ICA staff to perform site visits yearly that will include comparing paper files to the data entered into HMIS to check for data accuracy and completeness.

ICA HMIS Staff Role

* Review the data quality reports for each CoC.
* If a provider has data quality issues, forward the report to the provider, so they can fix their data.
* Review the provider list for each report. If there are missing or incorrect providers on the list, confirm those with the agency.
* Run specified data quality reports monthly\*.
* Run specified data quality reports quarterly\*.
* Assist funders with monitoring when appropriate and provide technical assistance regularly to non-funded HMIS participating agencies.
* Provide HMIS training to new users prior to giving access to the system.
* Provide ongoing HMIS training for existing end users.

Designated HMIS Agency Contact

* Review data quality reports sent to you by ICA HMIS Staff person(s).
* If you have data quality issues, correct them as soon as possible.
* Run data quality reports to check client data on a monthly basis.
* Compare paper files to data entered in HMIS regularly.
* Direct any HMIS questions to ICA HMIS Staff.

User Role

* Input required data fields accurately and in a current and timely manner.
* Review data quality reports sent to you by your Designated Agency HMIS Contact or ICA HMIS Staff.
* Correct data quality issues as soon as possible

7.3 DATA COMPLETENESS

All data entered in the HMIS must be complete. Completeness is the level at which a field has been answered in whole or in its entirety. Measuring completeness can ensure that client profiles are accurately answered in whole and that an entire picture of the client situation emerges. Partially complete or missing data (e.g., missing the SSN, missing the date of birth, missing information on disability or missing veteran status) can negatively affect the CoC’s ability to provide comprehensive care to clients. Incomplete data results in an inaccurate picture of the need in the CoC, directly affecting services in individual communities necessary to permanently house clients. It is every HMIS end user’s responsibility to report an accurate picture of populations served to facilitate accurate reporting and analysis.

The goal is to collect 100% of all data elements for all household members. However, the HMIS Advisory Committee recognizes that this may not be possible in all cases. Therefore, an acceptable range of null/missing and unknown/don’t know/prefers not to answer responses has been established, depending on the data element and the project type. Missing data elements are data elements that were either not collected or collected but were not entered into HMIS. Don’t know/prefers not to answer data elements are those data elements that were not collected because the client either doesn’t remember the information or prefers not to answer the question. Don’t know/prefers not to answer is from the clients’ perspective and is not used to denote that the information was not collected.

Participating agencies will be expected to record the most complete data possible. Only when a client prefers not to provide their information or their dependent’s personal information and the project funder does not prohibit it, it is permissible to enter incomplete client data.

Some required procedures to follow are:

* If a client prefers not to provide the remaining identifiable elements, record the answer as “prefers not to answer.”
* If a client’s record already exists in HMIS, the agency must not create a new alias or duplicate record. Client records entered under aliases or duplicate records may affect an agency’s overall data completeness and accuracy rates. The agency is responsible for any duplication of services that results from hiding the actual name under an alias.

7.4 DATA COMPLETENESS STANDARDS

* *Emergency Shelter projects:*All Universal Data Elements will be entered with an overall completeness rate of 95% or greater.
* *Outreach projects:* All Universal and Project Specific Data Elements (if HUD or SAMHSA funded) will be entered with an overall completeness rate of 90% or greater ***after client enrollment date.***
* *Permanent Supportive Housing projects (including HUD-VASH):*All Universal and Project Specific Data Elements will be entered with an overall completeness rate of 98% or greater.
* *Transitional Housing projects:*All Universal and Project Specific Data Elements will be entered with an overall completeness rate of 98% or greater.
* *Rapid Re-Housing projects:*All Universal and Project Specific Data Elements will be entered with an overall completeness rate of 98% or greater.
* *Prevention projects:* All Universal and Project Specific Data Elements will be entered with an overall completeness rate of 98% or greater.
* *HOPWA projects:* All Universal and Project Specific Data Elements will be entered with an overall completeness rate of 98% or greater.
* *Coordinated Entry projects:* All Universal Data Elements and Project Specific Data Elements will be entered with an overall completeness rate of 90% or greater.
* *Supportive Services Only projects:* All Universal Data Elements and Project Specific Data Elements will be entered with an overall completeness rate of 98% or greater.

7.5 DATA CONSISTENCY

ICA HMIS Staff will evaluate the quality of all HMIS Participating Agency data on the consistency of the data being entered. All Participating Agencies across the CoCs should work consistently to reduce duplication in HMIS by following workflow practices outlined in training. HMIS end users are trained to search for existing clients in the system, across multiple parameters, before adding a new client into the system. Client data can be searched by Client ID, Name, Social Security Number, and Client Alias. End users are trained to follow this protocol when adding a new client to the system.

Data consistency will ensure that data is understood, collected, and entered consistently across all projects in the HMIS. Consistency directly affects the accuracy of data; if an end user collects all the data, but they don't collect it in a consistent manner, then the data may not be accurate. All data in HMIS shall be collected and entered in a common and consistent manner across all projects. To that end, all end users will complete an initial training before accessing the live HMIS system.

ICA HMIS Staff will provide regular training, refresher courses, as well as updated data entry workflows and sample intake forms as a guide for quick reference when collecting and entering data to ensure that data is understood, collected, and entered consistently across all programs in the HMIS.

ICA HMIS Staff will review data entries in the database quarterly for duplicate entries and merge any duplicate client records found at this time. If a participating agency is consistently creating duplicate clients, the HMIS staff will contact the designated Agency Administrator to notify and address the end user creating the duplication, so future duplication can be avoided.

All HMIS Participating Agency client data should adhere to HMIS capitalization guidelines. HMIS end users are trained on the current method and style to enter client level data. For example, client names are entered with the first initial of the first and last name capitalized (i.e., First Last). No client name should be entered in any of the following ways:

* ALL CAPS
* all lower case
* Mix of lower- and upper-case letters
* Nicknames in the Name space (use the Alias box instead)

7.6 DATA ACCURACY

Accurate data ensures that the HMIS is the best possible representation of reality as it relates to persons experiencing homelessness and the programs serving them on a day-to-day basis. Accuracy can be difficult to assess as it depends on the client providing correct data and the intake worker’s ability to document and enter the data accurately. Accuracy is best determined by comparing records in the HMIS to paper records, or the records of another reliable provider. For example, an SSN in question can be compared to a paper case file or SSI benefit application. In-person interviews, with clients participating in projects who are utilizing the HMIS, are another method for assessing accurate data entry. Evaluation for accurate documentation of case management, service transactions and referrals in the HMIS can be assessed by client interviews. In-person interviews with clients may be coordinated with funders during HUD monitoring or performed individually with non-HUD funded Participating Agencies by HMIS staff, when appropriate.

Information entered in the HMIS needs to be valid, meaning it needs to accurately represent information on the participants of the homeless service projects contributing data to the HMIS implementation. Inaccurate data may be intentional or unintentional. In general, false, or inaccurate information is less desirable than incomplete information, since with the latter, it is at least possible to acknowledge the gap. Thus, it should be emphasized to clients and staff that it is better to enter nothing (or preferably “client doesn't know” or “prefers not to answer”) than to enter inaccurate information. To ensure the most up-to-date and complete data, data entry errors should be corrected monthly.

All data entered into the HMIS shall be a reflection of information provided by the client, as documented by the intake worker or otherwise updated by the client and documented for reference. Recording inaccurate information is strictly prohibited.

7.7 DATA ACCURACY STANDARD

|  |  |  |
| --- | --- | --- |
| **Data Quality Measurements: Accurate Data\***  | **Applicability of Standard by Project Type**  | **Max Allowed**  |
| Missing Entry/Exits  | All Projects  | 0%  |
| Incorrect Entry Type  | All Projects  | 0%  |
| Duplicate Entry/Exits  | All Projects  | 0%  |
| Future Entry/Exits  | All Projects  | 0%  |
| Missing Exit Dates | All Projects | 0% |
| Unknown Destinations  | All Projects  | 20% for CE, ES, and Outreach3% All Other Types |
| Children Only Households  | All Projects  | 0%  |
| Missing Head of Household  | All Projects  | 0%  |
| Missing Services and Referrals | PATH | 0%  |
| Service Dates fall outside of Entry and Exit Dates  | PATH | 0%  |

7.8 DATA TIMELINESS

Data shall be recorded in HMIS on a consistent and timely basis. Users shall strive for real-time, or close to real-time data entry. Real-time or close to real-time is defined by either immediate data entry upon seeing a client or data entry into the HMIS database within six calendar days.

7.9 BED/UNIT UTILIZATIONS RATES

One of the primary features of an HMIS is the ability to record the number of client stays or bed nights at a homeless assistance project. The count of clients in a project on a given night is compared to the number of beds reported in the Housing Inventory Count (HIC) to return the agency’s Bed Utilization percentage. The generally acceptable range of bed utilization rates for established projects is 65%- 105%.

|  |  |  |
| --- | --- | --- |
| **Project Types**  | **Lowest Acceptable Bed Utilization Rate**  | **Highest Acceptable Bed Utilization Rate**  |
| ES, TH, PSH, RRH  | 65%  | 105%  |

7.10 MONITORING PLAN

The HMIS Advisory Committee recognizes that the data produced from HMIS is critical to meet the reporting and compliance requirements for individual partner agencies and the entire HMIS implementation. As such, all HMIS partner agencies are expected to meet the data quality benchmarks described in this document.

To achieve this, the HMIS data will be monitored on a quarterly basis to quickly identify and resolve issues that affect the timeliness, completeness, consistency, and accuracy of the data. All monitoring will be done in accordance with the data quality monitoring plan, with full support of the CoC Governing Boards and the HMIS Advisory Committee.

The purpose of monitoring is to ensure that the agreed-upon data quality benchmarks are met to the greatest extent possible, and that data quality issues are quickly identified and resolved. To ensure that Participating Agencies have continued access to the expectations set forth in the data quality plan, the following protocol will be used:

1. The CoC Governing Boards and the HMIS Advisory Committee will have the ability to review and critique the Data Quality Plan draft prior to publication and will continue to provide input when updates are necessary.
2. Participating agencies will provide timely updates to the HMIS staff in their corresponding CoC regarding any changes to programs.
3. Data Quality reports will be reviewed at a minimum once a quarter by HMIS staff and senior staff at all HMIS participating agencies in the CoC.
4. HMIS staff and participating agencies throughout each CoC must work to prevent duplicate data.
5. HMIS staff will monitor the creation of duplicate client records within the system and correct at least quarterly.
6. Participating agencies must review hardcopy records and compare them to the HMIS data to ensure consistency.
7. HMIS will provide new end users with new user training and provide existing users with access to training throughout the year to reflect any system updates.
8. HMIS staff will assist programs within their service area in correcting data and updating information as needed.
9. Participating agencies that meet the data quality benchmarks will be periodically recognized by their respective HMIS staff.

7.11 DATA QUALITY PLAN ENFORCEMENT

ICA HMIS Staff will take the following steps to enforce the Data Quality Plan:

1. ICA HMIS staff will first provide additional in-person technical assistance for participating agencies that fail to meet the data quality benchmarks set forth in this document.
2. If corrective action is not taken, ICA HMIS Staff will send the HMIS Participating Agency a notice stating they are non-compliant with the standards set for data quality. The participating agency will be asked to submit a plan to the ICA HMIS Staff describing how they intend to improve their data quality to meet HMIS standards.
3. If a plan of action is requested, and is not submitted within the allotted time frame, the ICA HMIS staff may suspend all end user accounts under that project for a period no longer than 7 days.
4. After the suspension, end user accounts will be restored, and the HMIS Participating Agency will have the opportunity to correct data until the next month’s review and will follow the same process as before. ICA HMIS Staff will report the suspension to the HMIS Advisory Committee.
5. If the HMIS Participating Agency’s account needs to be suspended for a second time, the ICA HMIS Staff may suspend user accounts for up to 30 days. Should the problem persist, or if the participating agency fails to submit a written plan, ICA may suspend the participating agency’s ability to enter data into the HMIS, and will contact any appropriate state and federal funders, notifying these funders of the participating agency’s non-compliance with HMIS data entry mandates. ICA HMIS Staff will report the suspension to the HMIS Advisory Committee.

The ICA HMIS staff will investigate all potential violations of any security protocols. A participating agency’s access may also be suspended or revoked if serious or repeated violation(s) of HMIS Policies and Procedures occur by agency users. Any user found to be in violation of security protocols will be sanctioned which may include, but are not limited to:

* A formal letter of reprimand
* Suspension of system privileges
* Revocation of system privileges
1. See Appendix 1 for additional information about federal HMIS requirements. [↑](#footnote-ref-2)
2. Additional Wisconsin and Northern Illinois HMIS governance documents are found on the ICA website here: <https://icalliances.org/wisconsin-governance> [↑](#footnote-ref-3)
3. The Consumer Privacy Notice and HMIS Baseline Privacy Statement are found on the ICA website here: https://icanewengland.helpscoutdocs.com/article/282-vermont-hmis-governance [↑](#footnote-ref-4)
4. See Appendix 1 – Federal HMIS Requirements [↑](#footnote-ref-5)
5. See Appendix 2 – Data Quality Plan [↑](#footnote-ref-6)