Wisconsin Statewide and Northern Illinois

Homeless Management Information System

Policies and Procedures

Institute for Community Alliances

2023

Contents

1. Introduction

1.1 BACKGROUND

The Wisconsin Statewide and Northern Illinois Homeless Management Information System (HMIS) is a collaborative project of the four Wisconsin Continua of Care (CoC) – Balance of State, Dane, Milwaukee, and Racine, the Rockford/Winnebago/Boone/DeKalb Continuum of Care, known in this document as Northern Illinois Continua of Care, the Institute for Community Alliances (ICA), and participating Partner Agencies. 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 Wisconsin, local government entities and some private funders also require Partner Agency participation in HMIS.[1]

HMIS is an internet-based database that is used by homeless service organizations across Wisconsin to record and store client-level information about the numbers, characteristics and needs of homeless persons and those at risk of homelessness. HMIS enables service providers to measure the effectiveness of their interventions and facilitate longitudinal analysis of service needs and gaps within the CoCs and serves as the primary data management tool for their Coordinated Entry Systems. 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 Wisconsin is used to inform public policy decisions aimed at addressing and ending homelessness at local, state, and federal levels.

Bitfocus is the software vendor selected by the Wisconsin CoCs to administer the central server and HMIS software. ICA administers user and agency licensing, training, and compliance. Guidance for the implementation of Wisconsin and Northern Illinois' HMIS is provided by a broad-based advisory board that is committed to understanding the gaps in services to consumers of the human service delivery system to end homelessness.

This document provides the policies, procedures, guidelines, and standards that govern HMIS operations, as well as the responsibilities for Designated Agency HMIS Contacts and end users.[2]

1.2 HMIS BENEFITS

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

<u>Benefits for service providers</u>

- Provides online real-time information about client needs and the services available for homeless persons.

[1] See Appendix 1 for additional information about federal HMIS requirements.

[2] Additional Wisconsin and Northern Illinois HMIS governance documents are found on the ICA website here: https://icalliances.org/wisconsin-governance

- Assures confidentiality by providing information in a secured system.
- Decreases duplicative client intakes and assessments.
- 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 with other agencies and programs.
- Provides access to a statewide database of service providers, allowing agency staff to easily select a referral agency.
- Better able to define and understand the extent of homelessness throughout Wisconsin and Northern Illinois.
- Better able to focus staff and financial resources where services for homeless persons are needed the most.
- Better able to evaluate the effectiveness of specific interventions and programs, and services provided.

Benefits for homeless persons

- Intake information and needs assessments are maintained historically, reducing the number of times homeless persons must repeat their stories to multiple service providers.
- 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.
- HMIS data facilitates system improvement and provider accountability for client outcomes.

2. Requirements for Participation

2.1 PARTNER AGENCY REQUIREMENTS

Partner Agency Authorization to Access HMIS

The HMIS Lead Agency will review all requests for access from new potential Partner Agencies. Requests for HMIS access will be granted to agencies that have a business interest in the HMIS. The HMIS Lead Agency will take into consideration the agency's intent to contribute data into the system or use HMIS data for the following: homeless service provision, referrals to non-homeless services used by persons experiencing homelessness or data analysis.

To become a Partner Agency, the agency must complete the Participation Agreement Documents listed below.

Participation Agreement Documents

Partner Agencies must complete the following documents:

1. **Partnership Agreements** must be signed by each participating agency's executive director or their designee. The Institute for Community Alliances will retain the original

document. The participation agreement states the agency's commitment to adhere to the policies and procedures for effective use of HMIS.[3]

2. **Wisconsin User Agreements** list user policies and responsibilities and are electronically signed by each authorized user. An electronic or hard copy of the original document must be kept by the Partner Agency where the user is employed or volunteers.[4]

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

User License Eligibility

Users must be paid staff or official volunteers of a Partner Agency. An official volunteer must complete a volunteer application with the Partner Agency, undergo agency training, pass a criminal background check, and record volunteer hours with the agency. Individuals who are solely contracting with a Partner Agency are prohibited from receiving a user license. All users must be at least 18 years old. All users must undergo a criminal background check as detailed in the Agency Partnership Agreement. All users must complete training before access to the system is granted by ICA. ICA System Administrators will send all new user account information to the users work email. Users without a work email address must have their email address verified by their supervisor prior to receiving their new user account information.

Passwords

- Creation: ICA System Administrators will generate passwords for new users and communicate the password and login information to users.
- Use: The user will be required to change the password the first time they log onto the system. The password must be at least 8 characters and contain upper- and lower-case letters and at least one number and symbol. Passwords should not be able to be easily guessed or found in a dictionary. Passwords are the individual's responsibility and users cannot share passwords. Users may not keep written copies of their password in a publicly accessible location.
- Storage: Any passwords that are written down are to be stored securely and must be inaccessible to other persons. Users are not to store passwords on a personal computer for easier log on.
- Expiration: Passwords expire every 45 days. Users may not use the same password consecutively. Passwords cannot be re-used until 2 password selections have expired.
- Unsuccessful login: If a user unsuccessfully attempts to login four times, the User ID will be "locked out," and access permission will be revoked rendering the user unable to gain access for one hour. Users may contact System Administrators to have their password reset.

Tracking of Unauthorized Access

[3] The Partnership Agreement and Coordinated Services Agreement are found on the ICA website here: https://icalliances.org/wisconsin-governance.

[4] The Wisconsin User Agreement is found on the ICA website here: https://icalliances.org/wisp-user-agreement

Any suspicion of unauthorized activity should be reported to the Institute for Community Alliances HMIS staff as outlined under Section 3.10.

Client Consent to Share Data

Agencies are required to ensure clients know what data are 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.
2. Agency staff must be able to provide a copy of the HMIS Baseline Privacy Statement upon client request.[5]
3. Clients may elect to share or not share their information with HMIS participating agencies and CoC Data Partners.
4. Agencies may elect to use a signed release of information form with clients. Agencies that choose to implement a release of information must do so in a consistent manner with all agency clients. Agencies that use a release of information must use the most up-to-date Client Release of Information form made available on the ICA website.[6] The form allows the client to exercise their right to opt-out of data sharing in the cases where they have discretion.
5. 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.[7] Agencies may collect information for additional data elements. Agencies must maintain consistency with data collection and entry within each program.[8]

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 USER ROLES AND RESPONSIBILITIES

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.

[5] The Consumer Privacy Notice and HMIS Baseline Privacy Statement are found on the ICA website here: https://icalliances.org/wisconsin-governance.

[6] The Consumer Privacy Notice and HMIS Baseline Privacy Statement are found on the ICA website here: https://icalliances.org/wisconsin-governance.

[7] See Appendix 1 – Federal HMIS Requirements

[8] See Appendix 2 – Data Quality Plan

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

Designated Agency HMIS Contact Responsibilities

User Accountability at Agency

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

Program Information

1. 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.
2. 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 Board and/or the CoC in which the program operates.
3. Identify the assessment and reporting requirements for each program.

Agency Communication with ICA

1. Provide a single point of communication between users and HMIS staff at the Institute for Community Alliances.
2. Provide updated agency and program information to ICA and work with ICA System Administrators to properly set up each program in the HMIS.
3. Determine the appropriate user access role and communicate these requirements to the System Administrator. In all cases, the System Administrator will generate usernames and passwords within the administrative function of the software.

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 User Responsibilities

1. Take appropriate measures to prevent unauthorized data disclosure.
2. Report any security violations.
3. Comply with relevant policies and procedures.
4. Input required data fields accurately within 5 calendar days.
5. Ensure a minimum standard of data quality by accurately answering the Universal Data Elements and required program specific data elements for every individual entered into HMIS.
6. Inform clients about the agency's use of HMIS and secure the release of information needed for sharing client data.
7. Take responsibility for any actions undertaken with one's username and password.

8. Complete required training.
9. Read the Wisconsin and Northern Illinois HMIS newsletter.

Coordinated Entry or Service Referral User
Users who enter data in HMIS for the purposes of participating in their CoC's coordinated entry system or to make service referrals in HMIS are coordinated entry or service referral users. The training requirements and user fees associated with this type of user license may differ from those of a general user.

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 Wisconsin 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. 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 these training and data entry requirements.

Full participation and attention in all trainings attended is expected.

New User Training Requirements for General Users
All users are required to attend new user training with ICA prior to receiving access to the system.

Once a new user begins the HMIS New User Training Series, the user has 15 days to complete the training series, including associated forms and quizzes.

Every attempt will be made by HMIS Lead staff to assist users in successfully understanding HMIS data entry concepts. If a new user fails to successfully complete the data entry requirements after working with ICA staff directly, ICA staff may use their discretion to determine that the user is not capable of accurate and complete data entry and may refuse to issue or reissue the user a Wisconsin HMIS user license.

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 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.

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 may 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.

Report Training – Data Analysis License

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.

Coordinated Entry Training

Coordinated Entry Training is considered a separate training and is required separately by each CoC. Each 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 CoC. Agencies and users are responsible to check with their 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 by January 5th of the following year. To reactivate the license, the user must complete their training requirements.

New User Training Requirements for Agencies New to HMIS

The Executive Director, direct manager, and all users who are at the agency and interact with the program being entered into HMIS are required to attend new user training with ICA prior to the agency receiving access to the system.

Once the New user Training Series is started, each user has 15 days to complete the training series, including associated forms and quizzes.

Please note: the Executive Director and direct manager, must also review the relevant governance documents related to the agency responsibilities related to HMIS.

2.5 HMIS VENDOR REQUIREMENTS

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

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

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

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

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

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

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

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

2.6 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: 4Gig recommended (2 Gig minimum)

Monitor

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

Processor

- A Dual-Core processor is recommended

2.7 HMIS LICENSE FEES

Agencies may purchase licenses at any time.

Billing occurs in two situations.

1. Billing for licenses will occur once annually for the number of licenses the agency will utilize throughout the year, corresponding to the beginning of the next HMIS software contract period.
   a. Agencies will be notified in advance of when the invoices will be issued and, in that period, will have the opportunity to revise their assessed license count to match those in use. The annual fee will cover the invoiced year 4/1 - 3/31 and must be paid within 60 days following the date of the invoice. If a Partner Agency fails to pay their license fees by the stated due date, the agency's user licenses will be suspended until ICA receives the payment.
2. Billing for new licenses, additional license above the annually determined number, will incur the following quarter when the license has been added to the system. Agencies will be billed $300 for any new licenses above their annually determined number. This fee is subject to change without notice based on the cost incurred to the HMIS Lead for the additional license above the contracted amount with the Vendor.

Fees for Agencies Mandated to Use HMIS

Subsidized licenses are available to agencies who operate programs that contribute to the bed coverage in HMIS and/or are required by state or federal funding to enter their client information into the shared statewide HMIS. The amount of the subsidy provided is determined by the stated funding determination and the HMIS Lead's operating costs of the HMIS system. The subsidy amount is determined annually.

Fees for Agencies not Mandated to Use HMIS

Agencies that wish to use HMIS to track programs and services that are either not mandated by funding or that do not contribute to HMIS bed coverage on behalf of a respective CoC may, at the HMIS Director's discretion, be billed for the entire cost of an HMIS license. The full cost of a non-subsidized user license is $300 per year and subject to change annually as determined by the vendor.

Non-subsidized licenses are provided on a case-by-case basis if an agency or program is determined by the HMIS Lead to meet the requirements for access to HMIS.

Fees for Coordinated Entry and Service Referral Users
Funding for licenses associated with coordinated entry and service referral users will be determined by an agreement with each of the CoCs respective to their coordinated entry systems. Where a subsidy but the grantor is not provided, the full cost of the license will apply to the agency.

HMIS Reporting Platform Licenses
The reporting platform license is an add-on license available for HMIS users to facilitate data reporting. There is an amount charged for these licenses based on annual contractual amounts from the HMIS vendor. Agencies will be charged the contracted amount, with no additional fee added by the HMIS Lead. The current cost in 2023 is $120. This cost is subject to annual review.

Example of licensing fees:

At annual license invoicing:

6. 6 user licenses x $75 = $450 annual cost
7. 2 Looker licenses attached to the user license = $240

   Total annual license invoice $450 + $240 = $690

Throughout the year:

8. 1 user license added at a mid-point during the year

   Additional Invoice sent mid-year = $300

1 user license added at a mid-point, plus additional Looker License

   Additional Invoice sent mid-year = $420

Cost of Service to Grants Requiring Mandated Use of HMIS
Where possible the HMIS Lead will work with the grantor to directly charge the grantor for cost of service. Where not possible, funding shall be provided from agencies operating programs required by federal and state agencies to enter data into HMIS as needed to fully fund the operation of the HMIS. The amount charged will be a set dollar amount or a percentage allocation of the funding source, to be determined by ICA based upon various criteria.

2.8 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. The comparable database must meet the requirements set forth by HUD in the HMIS Comparable Database Manual.

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 Wisconsin 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. User violations do not expire. No regard is given to the duration of time that occurs between successive violations of the HMIS operation policies and procedures as it relates to corrective action.

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

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

- Third Violation – the user and Partner Agency will be notified of the violation in writing by ICA. ICA will notify the HMIS Advisory Board of the violation and convene a review panel made up of Advisory Board members who will determine if the user's license should be terminated. The user's license will be suspended for a minimum of 30 days, or until the Advisory Board review panel notifies ICA of their determination, whichever occurs later. If the Advisory Board determines the user should retain their user license, ICA will provide necessary training to the user and/or Partner Agency to ensure the violation does not continue. If users who retain their license after their third violation have an additional violation, that violation will be reviewed by the Advisory Board review panel.

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

Notifying the HMIS Lead Agency of a Violation

It is the responsibility of each Security Officer and User 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 wihmis@icalliances.org. The name of the person making the complaint will not be released from the HMIS Lead Agency if the individual wishes to remain anonymous.

Violations of Local, State or Federal Law

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

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

3. Privacy and Security

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

3.1 BASELINE PRIVACY POLICY

Upon request, clients must be able to access the *Baseline Privacy Policy* found below

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

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

Personal information must be 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 an agency using HMIS and provide the agency with their personal information.

Personal information may also be collected from:

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

Use and Disclosure of Personal Information

These policies outline how personal information may be used and disclosed by the Institute for Community Alliances (ICA) on behalf of the four Wisconsin Continua of Care, subject to oversight by the Wisconsin and Northern Illinois HMIS Advisory Board. Participating organizations may have separate privacy policies and that may allow different uses and disclosures of personal information. If clients access services at one of these organizations, they can request to view that agency's privacy and sharing policy.

The primary reason why personal information may be used or disclosed is to provide or coordinate services to individuals. To accomplish this goal, client data may be shared among HMIS-participating providers as well as with non-participating network partners—that is, agencies with which ICA has a written data sharing agreement. Through the HMIS Agency Agreement and ICA data sharing agreements, ICA will ensure that client data is used and disclosed only for purposes that improve service delivery for individuals.

Agencies collecting client information are required to notify clients that their personal information may be shared through the posting of the HMIS Consumer Notice.

Personal information will be used or disclosed without written client consent for activities described below. Clients must give consent before their personal information is used or disclosed for any purpose not described here:

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

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

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

4. 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.

5. 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.

6. For a law enforcement purpose (if consistent with applicable law and standards of ethical conduct) under any of these circumstances:
    - In response to a lawful court order, court-ordered warrant, subpoena, or summons issued by a judicial officer or a grand jury subpoena, if the court ordered disclosure goes through the Institute for Community Alliances and is reviewed by the Executive Director for any additional action or comment.
    - If the law enforcement official makes a written request for personal information. The written request must meet the following requirements:
        i. Be signed by a supervisory official of the law enforcement agency seeking the personal information.
        ii. State how the information is relevant and material to a legitimate law enforcement investigation.
        iii. Identify the personal information sought.
        iv. Be specific and limited in scope to the purpose for which the information is sought, and
        v. Be approved for release by the Institute for Community Alliances legal counsel after a review period of seven to fourteen days.
    - If it is believed that the personal information constitutes evidence of criminal conduct that occurred at the agency where the client receives services.
    - If the official is an authorized federal official seeking personal information for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to a foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 (threats against the President and others), and the information requested is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought.

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

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

requirements.

9. In the event of a public health emergency, personal information, including protected health information, may be disclosed to appropriate public health entities to support coordination measures to protect public health.

Inspection and Correction of Personal Information

Clients may inspect and receive a copy of their personal information maintained in HMIS. The agency where the client receives services will offer to explain any information that a client may not understand.

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

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

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

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

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

Limits on Collection of Personal Information

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

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

Limits on Partner Agency Use of HMIS Client Information

The Wisconsin and Northern Illinois 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 service in a way that discriminates against clients based on information the Partner Agency obtained from HMIS. Partner Agencies may not penalize a client based on historical data contained in HMIS.

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

Complaints and Accountability

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

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

3.2 HMIS INTERNAL PRIVACY SETTINGS

The Wisconsin and Northern Illinois 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.

3.3 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.

3.4 DATA REPORTING PARAMETERS AND GUIDELINES

Upon any request for HMIS System Data, ICA staff will adhere to the following principles for release of data:

- Only de-identified aggregated data will be released except as specified in the HMIS Baseline Privacy Notice.
- Program specific information used for annual grant program reports and program specific information included in grant applications is classified as public information. No other program specific information will be released without written consent.
- There will be full access to aggregate data included in published reports.
- Reports of aggregate data may be made directly available to the public.
- The parameters of the aggregated data, that is, where the data comes from and what it includes will be presented with each report.
- Data will be mined for agencies requesting reports on a case-by-case basis.
- Requests must be written with a description of specific data to be included and for what duration of time. Requests are to be submitted at least 30 days prior to the date the report is needed. Exceptions to the 30-day notice may be made.
- ICA reserves the right to deny any request for aggregated data. Final decisions will be made by the HMIS Director.

3.5 RELEASE OF DATA FOR GRANT FUNDERS

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

3.6 DATA SHARING EXTERNAL TO HMIS

Disclosure of client personal information to third parties requires a formal written agreement, authorized by the HMIS Advisory Board. 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 Board.

Third parties seeking client personal information from the Wisconsin and Northern Illinois 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 Board 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 Wisconsin website.

Any external sharing of client personally identifiable 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).

3.7 DATA CATEGORIZATION AND HANDLING

Proper data handling protocols depend on the nature of the information being transmitted or stored:

- Open Data: This is data that contains de-identified, client-level information. The data should be handled discretely, be stored out of sight, and may be transmitted via internal or first-class mail.

- Confidential Data: Confidential data contains personal identifying information, such as name, date of birth, and social security number. 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.
    - Electronic copies shall be magnetically overwritten when disposal is appropriate.
    - Encryption required for electronic transmission.

- <u>Aggregated Public Data</u>: Data that is published and available publicly. This type of data does not identify clients listed in the HMIS. Security controls are not required.

- <u>Unpublished Restricted Access Data</u>: 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.
    - 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.

<u>Partner Agency Record Retention Policy</u>
Partner agencies must have a written record retention policy that includes how printed HMIS records are destroyed.

3.8 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.

3.9 VIOLATION OF SECURITY PROCEDURES

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

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

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

3.10 PROCEDURE FOR REPORTING SECURITY INCIDENTS

Users and Designated Agency HMIS 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.

3.11 DISASTER RECOVERY PLAN

Bitfocus Disaster Recovery Plan

Wisconsin and Northern Illinois'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 WI HMIS Help Desk.

Standard Data Recovery

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

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

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

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

For power outage, HMIS is backed up via APC battery back-up units, which are connected via generator-backed up electrical circuits. For a system crash, a system restore will take four hours. There is potential for some small data loss (data that was entered between the last backup and when the failure occurred) if a tape restore is necessary. If the failure is not hard drive related, the data restore time will possibly be shorter as the drives themselves can be repopulated into a standby server.

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

Wisconsin and Northern Illinois HMIS Disaster Recovery Plan
The Institute for Community Alliances operates a regional approach to administering the Wisconsin and Northern Illinois HMIS. The main ICA Wisconsin and Northern Illinois HMIS office is located in Madison, Wisconsin. In the event of a localized emergency or disaster, ICA will shift responsibility for administering the HMIS and managing day-to-day operations of the system to an unaffected site.

4. Data Requirements

4.1 MINIMUM DATA COLLECTION STANDARD

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

The Designated Agency HMIS Contact must identify the assessments and requirements for each program. ICA will consult with the Designated Agency HMIS 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 Agency HMIS Contacts and posted on the Institute for Community Alliances' Wisconsin and Northern Illinois HMIS webpages. Designated Agency HMIS 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

Data quality is a term that refers to the reliability and validity of client-level data collected in the HMIS. It is measured by the extent to which the client data in the system reflects actual information in the real world. No data collection system has a quality rating of 100%. However, to meet the goals set forth by the four CoCs in the state of Wisconsin when presenting accurate and consistent information on homelessness, it is critical that the HMIS have the best possible representation of reality as it relates to persons experiencing homeless and the projects that serve them. Specifically, the goal is to record the most accurate, consistent and timely information in order to draw reasonable conclusions about the extent of homelessness and the impact on the homeless service system. To that end, the CoCs will collectively assess the quality of our data by examining characteristics such as timeliness, completeness, and accuracy.

See Appendix 2 for the complete Data Quality Plan.

4.4 DATA IMPORTS

While HMIS databases are required to have the capacity to accept data imports, ICA reserves the right to not allow data imports into Wisconsin and Northern Illinois' HMIS. Allowing data imports will impact data integrity and increase the likelihood of duplication of client files in the system.

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.

Confidential Data – contains personal identifying information.

Designated Agency HMIS Contact - the individual responsible for HMIS use at each partner agency. This includes running reports and verifying data entry is accurate and timely.

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

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

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

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

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

HMIS Vendor – the Wisconsin and Northern Illinois HMIS software vendor is Bitfocus. The HMIS vendor designs the HMIS and provides ongoing support to the System Administrators.

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

Open Data – does not contain personal identifying information.

Partner Agencies – the homeless service organizations that use HMIS.

System Administrators – staff at the Institute for Community Alliances who are responsible for overseeing HMIS users and use in Wisconsin. 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.

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. Appendix 1: Federal HMIS Requirements

6.1 Data Dictionary and Manual

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

The HMIS Data Dictionary is designed for HMIS vendors, HMIS Lead Agencies, and HMIS system administrators to understand all 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 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.

6.2 HMIS Regulations and Standards

The 2004 Data and Technical Standards Notice specifies describes 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. Appendix 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 are poor, funders may refuse to grant funding or reduce future funding. These funding cuts could negatively affect program(s) throughout the State of Wisconsin. As it is imperative that the data are 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 Wisconsin and Northern Illinois HMIS Governance 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

Wisconsin and Northern Illinois HMIS Advisory Board Role

- Have an ongoing relationship with the HMIS Users from across the state 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 policy 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 on-going HMIS training for existing end-users.

Designated Agency HMIS 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 question to ICA 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 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 Board recognizes that this may not be possible in all cases. Therefore, an acceptable range of null/missing and unknown/don't know/refused 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/refused data elements are those data elements that were not collected because the client either doesn't remember the information or refuses to answer the question. Don't know/refused 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 refuses to provide his or her or 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 refuses to provide the remaining identifiable elements, record the answer as "refused."
- 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 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 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 in 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 “refused”) than to enter inaccurate information. To ensure the most up-to-date and complete data, data entry errors should be corrected on a monthly basis.

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 Outreach 3% 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.

7.8 BED/UNIT UTILIZATION 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%

7.9 MONITORING PLAN

The HMIS Advisory Board 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 four CoC Governing Boards and the HMIS Advisory Board.

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 Board 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.

7.10 DATA QUALITY PLAN ENFORCEMENT

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

3. 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.
4. If corrective action is not taken, ICA HMIS staff will send the HMIS participating agency a notice stating they are noncompliant 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.
5. 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.
6. 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 Board.
7. 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 Board.

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