NORTH DAKOTA HOMELESS MANAGEMENT INFORMATION SYSTEM

Policies and Procedures

Institute for Community Alliances
September 2018

Table of Contents

1 Introduction 3
1.1 HMIS Benefits 3
2 Requirements for Participation 5
2.1 Responsibility of the HMIS User 5
2.2 Partner Agency Requirements 5
2.3 User Training Requirements 8
2.4 HMIS User Levels 9
2.5 HMIS Vendor Requirements 11
2.6 Minimum Technical Standards 11
2.7 HMIS License Fees 12
2.8 HMIS Operating Policies Violation 12
3 Privacy and Security 14
3.1 Data Assessment and Access 14
3.2 Data Reporting Parameters and Guidelines 15
3.3 Release of Data for Grant Funders 15
3.4 Baseline Privacy Policy 16
3.5 Use of a Comparable Database by Victim Service Providers 19
3.6 User Conflict of Interest 20
3.7 Security Procedure Training for Users 20
3.8 Violation of Security Procedures 20
3.9 Procedure for Reporting Security Incidents 20
3.10 Disaster Recovery Plan 20
4 Data Requirements 22
4.1 Minimum Data Collection Standard 22
4.2 Provider Naming Convention 22
4.3 Data Quality Plan 22
4.4 Data Imports 22
4.5 HMIS Data Protections 22
5 Glossary 24
6 Appendix 1: Data Dictionary and Data Manual 26
7 Appendix 2: Data Quality Plan 27
7.1 Goals of the Data Quality Plan 27
7.2 Data Quality Plan and Responsibilities 27
7.3 Data Completeness 28

7.4 Data Completeness Standards 29
7.5 Data Consistency 29
7.6 Data Accuracy 30
7.7 Data Accuracy Standard 32
7.8 Data Timeliness 32
7.9 Bed/Unit Utilization Rates 32
7.10 Monitoring Plan 32
7.11 Data Quality Plan Enforcement 33
8 Acknowledgement of Receipt of North Dakota HMIS Policy and Procedures, Privacy Notice, and Data Quality Plan 35

1 Introduction

The North Dakota Homeless Management Information System (HMIS) is a collaborative project of the North Dakota Coalition of Homeless People, the Institute of Community Alliances, and participating Partner Agencies. HMIS is an internet-based database that is used by homeless service organizations across North Dakota to record and store client-level information about the numbers, characteristics, and needs of homeless persons and those at risk of homelessness. WellSky Community Services administers the central server and HMIS software, and ICA administers user and agency licensing, training and compliance.

HMIS enables service providers to measure the effectiveness of their interventions and facilitate longitudinal analysis of service needs and gaps within the CoC. 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 North Dakota is used to inform public policy decision aimed at addressing and ending homelessness at local, state, and federal levels.

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.

1.1 HMIS Benefits

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

Benefits for service providers

- Provides online real-time information about client needs and the services available for homeless persons.
- Assures confidentiality by providing information in a secured system.
- Decreases duplicative client intakes and assessments.
- 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 North Dakota.
- 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 intervention 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 streamlined.

2 Requirements for Participation

2.1 Responsibility of the HMIS User

Designated Agency HMIS Contact

1. Provide updated agency information to ICA for update in HMIS.
2. Ensure that the participating agency obtain a unique user license for each user at the agency who will be using HMIS.
3. Maintain a minimum standard of data quality by ensuring the Universal Data Elements are complete and accurate for every individual served by the agency and entered into HMIS.
4. 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 North Dakota Coalition for Homeless People.
5. Ensure agency staff persons receive required HMIS training, review the North Dakota HMIS Policies and Procedures, the Agency Partnership Agreement, and any agency policies which impact the security and integrity of client information.
6. Ensure that HMIS access is granted only to staff members that have received training, have completed the North Dakota HMIS User Policy Code of Ethics and Responsibility Statement, and are authorized to use HMIS.
7. Notify all user at their agency of interruptions in service.
8. Provide a single point of communication between user and HMIS staff at the Institute for Community Alliances.
9. Administer and monitor data security policies and standards, including:
    a. User access control;
    b. The backup and recovery of data; and
    c. Detecting and responding to violations of the policies and procedures or agency procedures.

Users

1. Take appropriate measures to prevent unauthorized data disclosure.
2. Report any security violations.
3. Comply with relevant policies and procedures.
4. Input required data fields accurately within 5 calendar days.
5. Ensure 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 the required training
9. Read the North Dakota HMIS News email newsletter.

2.2 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 prevention service provision, referrals to non-homeless services uses by persons experiences 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. **North Dakota HMIS Agency Agreement** must be signed by each participating agency's executive director. The Institute for Community Alliances will retain a digital copy of the agreement and the Participating Agency will retain the original document. The agency agreement states the agency's commitment to adhere to the policies and procedures for effective use of the HMIS.
2. **North Dakota User Policy Code of Ethics and Responsibility Statement** lists the policies and responsibilities required by the user. These are signed by the user and are retained by the Institute for Community Alliances. An electronic or a hard copy must be kept by the originating agency.

User Access to the System

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

The Designated Agency HMIS Contact and all users must complete training before access to the system is granted by ICA.

User Requirements

User 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. Individuals who are solely contracting with a Partner Agency are prohibited from receiving a user license. All user must be at least 18 years old.

Users who are also Clients Listed in HMIS

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

Passwords

- Creation: Passwords are automatically generated from the system when the user is created. ICA will communicate the system-generated password to the user in the event the agency does not have a user with the agency administrator access.
- Use: The user will be required to change the password the first time they log onto the system. The password must be at least 8 characters and alphanumeric. Passwords should not be able to be easily guessed or found in a dictionary. Passwords are the individual's responsibility and

users cannot share passwords. Users may not keep written copies of their password in a publicly accessible location.

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

Inputting Data

Agencies participating in the HMIS must meet the minimum data entry requirements established under the most recently HMIS Data Standards.

Tracking of Unauthorized Access

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

Designated Agency HMIS Contact

The person is responsible for ensuring new agency staff persons are trained on how to use the HMIS by the System Administrators, and for ensuring that new staff are aware of any agency or program specific data entry requirements.

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

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 ensuring compliance with applicable security standards and maintaining the security of HMIS for their agency.

User Role: Agency Administrator

Agencies with 5 or more users must designate one person to designate one person to be the Agency Administrator. This person may also be the Designated Agency HMIS Contact. Agencies with fewer than 5 users may forego designated an Agency Administrator. ICA HMIS Staff will perform Agency Administrator responsibilities for these agencies.

The Agency Administrator will be responsible for resetting passwords and monitoring HMIS access by users at their agency. The user assigned as Agency Administrator must also act as the Designated Agency HMIS Contact.

Client Informed Consent and Release of Information

In addition to posting the HMIS Consumer Notice, agencies must obtain client consent prior to sharing client data with other agencies when data sharing is appropriate for client service delivery. Agencies are required to ensure client know what data is being collected about them and be given the opportunity to

make choices about what personal and program related information is shared in HMIS and with whom the data is shared. Agencies will use the Client Informed Consent and Release of Information form on the ICA website. The form requires clients to authorize the electronic sharing of their personal information and allows for clients to have more control over their own information. Agencies are required to obtain client consent. Clients have the right to refuse any level of shared data.

Data Protocols

Agencies may collect information for data elements in addition to minimally required data elements established by the North Dakota Coalition for Homeless People in accordance with HUD. Agencies must maintain consistency with data collection and entry within each program.

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.

2.3 User Training Requirements

New User Training Requirements

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

Once a new user begins the HMIS New User Training Course, the user has 15 days to complete the training course and all required assignments. ICA Staff will review the user's homework and determine if corrections are needed. User will have an additional 15 days to make all corrections. If the user fails to complete all requirements within 30 days, the user will need to retake the training course. ICA staff may determine that a new user failed to grasp the necessary data entry concepts based on the quality of the user's homework. ICA staff may use their discretion to require new users to repeat user training. If a new user fails to successfully complete the homework requirements for data entry after repeated attempts, ICA staff may use the 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 North Dakota HMIS user license.

Included in and in addition to the New User Training Course, users will be required to take program and/or project specific training related to the programs and projects administered by their agency.

In regard to Coordinated Entry, it is the responsibility of the agency to inform the user of the training curriculum and requirements for an agency and/or user's participation in Coordinated Entry in HMIS. Where provided by the CoC, ICA will host a link to those requirements. ICA will provide the HMIS specific workflow and report trainings.

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

Users are excepted to fully participate in all trainings attended. If a user misses more than 10 minutes or 10 percent (whichever is greater) of a training, the user will not receive credit for completing the training.

Ongoing User Training Requirements
All users are required to attend annual security training to retain their user license.

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

Users are expected to fully participate in all training attended. If a user misses more than 10 minutes or 10 percent (whichever is greater) of a training, the user will not receive credit for completing the training.

The HMIS Lead Agency will suspend user licenses from users who do not complete their annual training requirements by December 31 of the following year. To activate the license, the user must complete their training requirements.

2.4 HMIS User Levels

HMIS User Roles are listed on the ICA Website. HMIS User Roles

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

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

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

Volunteer

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

Agency Staff

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

Case Manager I

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

Case Manager II

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

Case Manager III

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

Agency Administrator

Users may access all ServicePoint screens and modules. Agency Administrators are responsible to reset the passwords of users at their agency. Agency Administrators may add/remove users and edit agency and program data for all providers on their provider tree.

Executive Director

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

System Operator

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

System Administrator I

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

System Administrator II

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

2.5 HMIS Vendor Requirements

Physical Security
Access to the 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
User many 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 database 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 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 7, 8, or 10
- The most recent version of Firefox, Google Chrome, or Safari. No additional plug-in is required. It is recommended that your browser have a 128 cipher / encryption strength installed. The browser's cache should be set to "Check for new version of the stored pages: Every visit to page."
- A broadband Internet connection or LAN connection. Dial-up modem connections are not sufficient.

- Virus protection updates.
- Mobile devices used for HMIS data entry must use the Mozilla Firefox, Google Chrome or Able Safari Internet browsers. Apple Safari must be used on the latest version of iOS.

Additional Recommendations

Memory

- Windows 7, 8, or 10: 4 Gig recommended (2 Gig minimum)

Monitor

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

Processor

- A Dual-Core processor is recommended.

2.7 HMIS License Fees

Each July, the North Dakota Continuum of Care for Homeless People will invoice agencies for their HMIS licenses. Agencies will be invoiced in tiered manned based on the number of licenses an agency has allocated to them.

- 1 license - $225
- 2 – 5 licenses - $200
- 6 or more licenses - $175

2.8 HMIS Operating Policies Violation

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

- First Violation – the user and the 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 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 North Dakota Coalition of Homeless People Steering Committee of the violation during the next scheduled Steering Committee meeting following the violation.

- Second Violation – the user and the 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, 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 North Dakota Coalition of Homeless People Steering Committee of the violation during the next scheduled Steering Committee meeting following the violation.

- Third Violation – the user and Partner Agency will be notified of the violation in writing by ICA. ICA will the North Dakota Coalition of Homeless People Steering Committee of the violation and convene a review panel made of the Steering Committee members who will determine if the user's license will be suspended for a minimum of 30 days or until the Steering Committee review panel notified ICA of their determination, which ever occurs later. If the Steering Committee 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 user retain their license after their third violation have an additional violation, that violation will be reviewed by the Steering Committee review panel.

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

Notifying the HMIS Lead Agency of a Violation

It is the responsibility of each Designated Agency HMIS Contact and general 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 the potential violation must include the User and Partner Agency name and the 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 ndhmis@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, include the collection, maintenance, use, disclosure, transmission and destruction of data, comply with HMIS privacy, security, and confidentiality policies and procedures. When a privacy or security standard conflicts with other Federal, state and local laws to which the Partner Agency must adhere, the Partner Agency must contact ICA to collaboratively update the applicable policies for the partner agency to accurately reflect the additional protections.

3.1 Data Assessment and Access

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

Shared Data
Shared data is unrestricted information that has been entered by one provider and is visible to other providers using HMIS. North Dakota's HMIS is designed as a shared system that defaults to allow shared data.

Data that is Not Shared
Information entered by one provider that is not visible to other providers using HMIS. Programs that serve individuals with HIV/AIDS, provide services to unaccompanied minors, or legal services must enter not shared data. Individual client records can be not shared at the client's request.

Procedures for transmission and storage of data

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

Whenever confidential data is accessed:

- Hard copies shall be shredded when disposal is appropriate. Hard copies shall be stored in a secure environment that is inaccessible to the general public or staff not requiring access.
- Hard copies shall not be left tout in the open or unattended.
- Electronic copies shall be stored only where the employee can access the data.
- Electronic copies shall be stored where a password is required to access the data if on shared server space.

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

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

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

Procedures for Transmission and Storage of Data

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

3.2 Data Reporting Parameters and Guidelines

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

Principles for Release of Data

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

3.3 Release of Data for Grant Funders

Entities providing funding to agencies or programs required to use HMIS will not have automatic access to HMIS. Access to HMIS will only be granted by ICA when there is a voluntary written agreement in

place between the funding entity and the agency or program. Funding for any agency or program using HMIS cannot be contingent upon establishing a voluntary written agreement allowing the funder HMIS access.

3.4 Baseline Privacy Policy

Collection of Personal Information

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

- To provide or coordinate services for clients.
- To find programs that may provide additional client assistance.
- To comply with government and grant reporting obligations.
- To assessment 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 an agency using HMIS and provide the agency with their personal information.

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

Personal information may also be collected from:

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

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

Use and Disclosure of Personal Information

These policies explain why an agency collects personal information from clients. Personal information may be used or disclosed for activities described in this part of the notice. Client consent to the use or disclosure of personal information for the purposes described in this notice, and for reasons that are compatible with purposes described in this notice, but not listed, is assumed. Clients must give consent before their personal information is used or disclosed for any person 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 have separate privacy policies and that may allow different uses and disclosures of the information. If the clients access services at one of these other organizations, they will be notified of the agency's privacy and sharing policy. {OPTIONAL}*

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

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

4. For academic research conducted by an individual or institution that has a formal relationship with the Institute for Community Alliances. The research must be conducted by an individual employed by or affiliated with the organization or institution. All research project must be conducted under written research agreement approved in writing by the Designated Agency HMIS Contact or Executive Director. The written research agreement must:
    - Establish 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 the terms and conditions of the written research agreement, and
    - Be substituted, when appropriate, by Institutional Review Board, Privacy Board, or other applicable human subjects' protection institution approval.

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

6. To avert a serious threat to health or safety if:
    - the use or disclosure is necessary to prevent or lessen a serious or imminent threat to the health or safety of an individual or the public, and
    - the use or disclosure is made to a person reasonable able to prevent or lessen the threat, including the target of the threat.
7. 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 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 of 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 judgement.
8. For a law enforcement purpose (if consistent with applicable law and standards of ethical judgement) under any of these circumstances:
    - In response to 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 person for 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 of 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 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.

9. 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.
10. 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 agency where the client received 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 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 complied 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 and 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, or contract or another obligation.

Limits on Partner Agency Use of HMIS Client Information

The North Dakota HMIS is a shared data system. The system allows Partner Agencies to share client information in order to coordinate services for clients. However, Partner Agencies may not limit client service or refuse to provide service in a way that discriminates against clients based on information the Partner Agency obtained from HMIS. Partner Agencies may not penalize a client based on historical data contained in HMIS.

Youth providers serving clients under the age of 18 must maintain HMIS 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 about Accountability

Questions or complaints about the privacy and security policies and practices may be submitted to the agency where the client received 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 Directors. If there is no resolution, the North Dakota Coalition of Homeless People Steering Committee will oversee the 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. User must receive and acknowledge receipt of this privacy notice.

3.5 Use of a Comparable Database by Victim Service Providers

Victim service providers, private non-profit 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 funder 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 datable that can use collected client-level data over time and generate unduplicated aggregated reports based on the client information entered into the database. The reports are generated by a comparable database must be accurate and provide the same information as the reported generated by HMIS.

3.6 User Conflict of Interest

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

3.7 Security Procedure Training for Users

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

3.8 Violation of Security Procedures

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

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

Any agency that is found to have consistently and/or flagrantly violated security procedures may have their access privileges suspended or revoked. All sanctions are imposed by the ICA HMIS Staff. All sanction may be appealed to the North Dakota Coalition for Homeless People Steering Committee.

3.9 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.

3.10 Disaster Recovery Plan

<u>Wellsky Community Services Disaster Recovery Plan</u>

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

- Database tape backups occur nightly

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

4 Data Requirements

4.1 Minimum Data Collection Standard

Partner Agencies are responsible for asking all clients at 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 elements in each assessment are highlighted with an asterisk (*) by the item indicated 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 the Designated Agency HMIS Contacts and posted on the Institute for Community Alliances North Dakota HMIS webpage. 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 be must be named so they accurately reflect the type of service carried out 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 extend to which the client data in the system reflects actual information in the real world. No data collection system as a quality rating of 100%. However, to meet the goals set forth by the North Dakota Coalition for Homeless People when presenting accurate and consistent information on homelessness, it is critical that the HMIS have the best possible representation of reality as it relations to the persons experiencing homelessness and the projects that serve them. Specifically, the goal is the record the most accurate, consistent and timely information in order to draw reasonable conclusions about the extent of homelessness and the impact on homeless service system. To that end, the CoC will collectively assess the quality of our data by examining characteristics such as timeliness, completeness, and accuracy.

See Appendix 7 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 not to allow data imports into North Dakota's HMIS. Allowing data imports will impact data integrity and increase the likelihood of duplication of client files in the system.

4.5 HMIS Data Protections

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.

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

North Dakota Coalition for Homeless People Steering Committee – the group of Coalition members who are responsible for approving and implementing the HMIS Policies and Procedures, and for working to make improvements to North Dakota 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 North Dakota's HMIS software vendor is Wellsky Community Services. 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 North Dakota. 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 Appendix 1: Data Dictionary and Data Manual

The HMIS Data Standards Manual is intended to serve as a reference and provide basic guidance on HMIS data elements for the CoC, 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 the of the data elements required in an HMIS, data collection and function for 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.

The current HMIS Data Dictionary and Data Manual can be found at:
https://www.hudexchange.info/resource/3824/hmis-data-dictionary/

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 Longitudinal System Analysis, 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 grant funding or reduce future funding. The funding cuts could negatively affect program(s) throughout the State of North Dakota. 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 in order to ensure all reports are complete, consistent, accurate, and timely.

7.1 Goals of the Data Quality Plan

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 also benefit from participating in this process by:

- Requiring less corrections right before reports are due, because data will be cleaned up regularly.
- Providing access to more up-to-date information to inform program decision, monitor client progress, and inform stakeholders about programs.
- Implementing changes when needed and measuring progress against goals

7.2 Data Quality Plan and Responsibilities

North Dakota Coalition for Homeless People Steering Committee

- 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 the 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 is 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 HMIS 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 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 staff.

User Role

- Input required data fields accurately and in 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 into 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 client. 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 ultimate goal is to collect 100% of all data elements for all household members. However, the North Dakota Coalition for Homeless People Steering Committee recognized that this may not be possible in all cases. Therefore, an acceptable range of null/missing and unknown/don't known/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 by for 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 procedure to follow are:

- If a client refuses to provide the remaining identifiable elements, record the answer as "refused".
- If the client's record already exists in HMIS, the agency must not create a new alias or duplicate record. Client records 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.

Note: A client may not wish to provide information to HMIS. That is their right and an HMIS Participating Agency cannot deny services to any client refusing inclusion in HMIS. However, in order for HUD funded providers to accurately complete reporting for their projects, either a De-identified client must be created in HMIs or the client's information and services must be tracked on paper.

7.4 Data Completeness Standards

- *Emergency Shelter projects*: All Universal Data Elements (if HUD funded) will be entered with an overall completeness rate of 95% or greater.
- *Outreach Projects*: All Universal and Project Specific Data Elements (if HUD funded) will be entered with an overall completeness rate of 90% or greater ***after client enrollment date***
- *Permanent Supportive Housing projects*: All Universal and Project Specific Data Elements will be entered with an overall completeness rate of 98% or greater.
- *Transitional Housing project*: 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 and Project Specific Data Elements will be entered with an overall completeness rate of 98% or greater.
- *Supportive Services Only projects*: All Universal 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 processes outlined in training.

HMIS 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 of 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 an entered in a common and consistent manner across all projects. To that end, all end user will complete an initial training before accessing the live HMIS system.

ICA HMIS staff will provide regular training, refresher courses, as well as updated 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 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 user 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 current data and the intake worker's ability to document and enter the data accurately. Accuracy is best determined by comparing record in HMIS to paper records, or the records of another reliable provider. For example, a SSN in question can be compared to a paper case file or SSN 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 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 into 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 is better to enter nothing (or 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	Data Quality Report Name	Applicability of Stand by Project Type	Max Allowed
Missing Entry/Exits	Data Completeness	All Projects	0%
Incorrect Entry Type	Data Completeness	All Projects	0%
Duplicate Entry/Exits	Data Completeness	All Projects	0%
Future Entry/Exits	Data Completeness	All Projects	0%
Missing Exit Dates	Unexited Clients Exceeding Max Length of Stay	All Projects	0%
Unknown Destinations	Data Completeness	All Projects	20% for ES 20% for Outreach 3% All Other Project Types
Children Only Households	Data Completeness	All Projects	0%
Missing Head of Household	Data Completeness	All Projects	0%

7.8 Data Timeliness

Data shall be recorded in HMIS on a consistent and timely basis. Users shall strive for real-time or as 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 within five (5) calendar days.

7.9 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 rate for established projects is 75%-105%

Project Type	Lowest Acceptable Bed Utilization Rate	Highest Acceptable Bed Utilization Rate
Emergency Shelter	75%	105%
Transitional Housing	80%	105%
Permanent Supportive Housing	85%	105%
Rapid Re-Housing	80%	105%

7.10 Monitoring Plan

The data produced from HMIS is critical to meet the reporting and compliance requirements for individual partner agencies and the HMIS implementation as a whole. 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 monthly 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 the full support of the North Dakota Coalition for Homeless People.

To ensure that service providers have continued access to the expectations set forth in the data quality plan the following protocol will be used:

1. Data Quality Plan will be published on ICA's website.
2. ICA will make available by the **15th of each month** data quality reports for the purposes of facilitating compliance review by participating agencies.
3. Participating Agencies will have **10 days** to correct the data.
4. The North Dakota Coalition for Homeless People's Steering Committee will review participating agency data quality reports for compliance with data quality benchmarks. The Committee will work with ICA to identify training needs to improve data quality.

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

1. The North Dakota Coalition for Homeless Persons 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 regarding any changes to programs.
3. Data Quality reports will be reviewed a minimum once a month by HMIS staff and senior staff at all HMIS participating agencies in the CoC.
4. HMIS staff and participating agencies throughout the 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 hard copy records and compare them to HMIS data to ensure accuracy.
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 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 that 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 North Dakota 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 North Dakota Coalition of Homeless People Steering 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 a problem persist, or in the event that the participating agency fails to submit a written plan, ICA may suspend the participating agency's ability to enter data into 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 North Dakota Coalition of Homeless People Steering 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

8 Acknowledgement of Receipt of North Dakota HMIS Policy and Procedures, Privacy Notice, and Data Quality Plan

The North Dakota HMIS Policy and Procedures, Privacy Notice and Data Quality plan contains important information regarding the expectations of agencies that use the North Dakota Homeless Information Management System.

_____ I acknowledge that I have received a copy of the North Dakota HMIS Polices and Procedures, Privacy Notice and Data Quality Plan. I understand that it is my responsibility to read and comply with these policies contained in this plan as well as any revisions made to it. I also understand that if I need additional information, or if there is anything that I do not understand in the Plan, I should contact my Designated HMIS Agency Contact for clarification.

_____ I understand that this Plan reflects policies, practices, and procedures in effect on the date of publication and that it supersedes any prior plan. I further understand that rules, policies, expectations, referred to in the Plan are evaluated and may be modified at any time, with or without notice. I acknowledge that the Plan will be updated once per year and it is my responsibility to be aware of and adhere to the changes of the Plan as they occur.

Signature:_____ Date: _____

Print Name: _____

Agency: _____