North Dakota-500
Statewide Continuum of Care

Homeless Management Information System Policies and Procedures

CoC Board Approval: April 19, 2021
CoC Membership Approval: May 5, 2021

Next Review: April 2022

I. Introduction

The North Dakota Homeless Management Information System (HMIS) is a collaborative project of the North Dakota Continuum of Care (herein ND CoC), the HMIS Lead Agency (herein HMIS LA), and participating Partner Agencies (herein Agencies/Agency). 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 persons at-risk of and experiencing homelessness. WellSky Community Services (herein WellSky) administers the central server and HMIS software, and the HMIS LA 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 clients 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.

A. HMIS Benefits

Use of the HMIS provides numerous benefits for service providers, persons at-risk of and experiencing homelessness, and the state of North Dakota.

1. Benefits for service providers:
    a. Provides online real-time information about client needs and the services available for persons at-risk of and experiencing homelessness.
    b. Assures confidentiality by providing information in a secured system.
    c. Decreases duplicative client intakes and assessments.
    d. Tracks client outcomes and provides a client history.
    e. Generates data reports for local use and for state and federal reporting requirements.
    f. Facilitates the coordination of services within an agency and with other agencies and programs.
    g. Provides access to a statewide database of service providers, allowing agency staff to easily select a referral agency.
    h. Better able to define and understand the extent of homelessness throughout North Dakota.
    i. Better able to focus staff and financial resources where services for persons at-risk of and experiencing homelessness are needed the most.
    j. Better able to evaluate the effectiveness of specific intervention, programs, and services provided.

2. Benefits for persons at-risk of and experiencing homelessness:
    a. Intake information and needs assessments are maintained historically, reducing the number of times persons at-risk of and experiencing homelessness must repeat their stories to multiple service providers.
    b. The opportunity to provide intake and life history one time demonstrates that service providers consider the person's time valuable and restores some of the client's dignity.
    c. Multiple services can be easily coordinated and streamlined.

II. Requirements for Participation

A. Responsibility of the HMIS Agency

1. Designated Agency HMIS Contact
    a. Provide updated agency information to the HMIS LA to update in HMIS.
    b. Ensure that the Agency obtains a unique user license for each user at the Agency who will be using HMIS.
    c. Work with the HMIS LA to communicate with the Agency when users are unresponsive to requests from the HMIS LA.
    d. 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.
    e. 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.
        - Administer and monitor data security policies and standards, including detecting and responding to violations of the policies and procedures or agency procedures.
2. Users
    a. Take appropriate measures to prevent unauthorized data disclosure.
    b. Report any security violations.
    c. Comply with relevant policies and procedures.
    d. Input required data fields accurately within five calendar days.
    e. Ensure minimum standard of data quality by accurately answering the Universal Data Elements and required Program Specific Data Elements for every individual entered in HMIS.
    f. Inform clients about the agency's use of HMIS and secure the Release of Information (ROI) needed for sharing client data.
    g. Take responsibility for any actions undertaken with one's username and password.
    h. Complete the required training.
    i. Read the North Dakota HMIS News email newsletter.

B. Partner Agency Requirements

1. Partner Agency Authorization to Access HMIS

    a. The HMIS LA will review all requests for access from new potential agencies. Requests for HMIS access will be granted to agencies that have a business interest in the HMIS. The HMIS LA 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 used by persons experiencing homelessness, or data analysis.

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

2. Participation Agreement Documents. Agencies must complete the following documents:

    a. North Dakota HMIS Agency Agreement must be signed by each Agency's executive director. The HMIS LA will retain a digital copy of the agreement and the 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.

    b. 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 HMIS LA. An electronic or a hard copy must be kept by the originating Agency.

3. User Access to the System

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

    b. All users must complete training before access to the system is granted by the HMIS LA.

4. User Requirements: Users must be paid staff or official volunteers of an Agency. An official volunteer must complete a volunteer application with the Agency, undergo Agency training, and record volunteer hours with the Agency. Individuals who are solely contracting with an Agency are prohibited from receiving a user license. All users must be at least 18 years old.

5. 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 HMIS LA will run the audit trail report to determine if there was an infraction.

6. Passwords

    a. Creation: Passwords are automatically generated from the system when the user is created. The HMIS LA will communicate the system-generated password to the user.

b. Use: The user will be required to change the password the first time they log onto the system. The password must be at least eight 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.

c. 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.

d. Expiration: Passwords expire every 45 days. Users may not use the same password consecutively. Passwords cannot be re-used until two password selections have expired.

e. Unsuccessful logon: If a user unsuccessfully attempts to log-on three 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.

7. Inputting Data: Agencies participating in the HMIS must meet the minimum data entry requirements established under the most recent HMIS Data Standards.
8. Tracking of Unauthorized Access: Any suspicion of unauthorized activity should be reported to the HMIS LA.
9. Designated Agency HMIS Contact
    a. This person is responsible for ensuring new agency staff persons are trained on how to use the HMIS by the HMIS LA and for ensuring that new staff are aware of any agency or program specific data entry requirements.
    b. The Designated Agency HMIS Contact must identify the data element requirements for each project and work with the HMIS LA to properly set up each project in the HMIS.
10. Designated Agency Security Officer
    a. Each Agency must designate a Security Officer. The Security Officer must be a current HMIS User and may also be the Designated Agency HMIS Contact.
    b. The Security Officer is responsible for ensuring compliance with applicable security standards and maintaining the security of HMIS for their agency.
11. 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 clients 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 ROI form on the HMIS LA 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. Users are required to complete the ROI data in the client's record in HMIS to indicate the date the release was signed, whether the client consented to the release, and the date the release

expires. Additionally, users are required to upload the completed ROI to the client's record in HMIS.

12. Data Protocols: Agencies may collect information for data elements in addition to minimally required data elements established by the CoC in accordance with HUD. Agencies must maintain consistency with data collection and entry within each program.
13. Agency Relationship with the HMIS Vendor: Agencies are prohibited from directly contacting the HMIS vendor to request custom database work. Any such request must be made through the HMIS LA.

C. User Training Requirements

1. New User Training Requirements

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

    b. Once a new user begins the HMIS New User Training Course, the user has 30 days to complete the training course and all required assignments. The HMIS LA will review the user's test case and determine if corrections are needed. The 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 new user training course. The HMIS LA may determine that a new user failed to grasp the necessary data entry concepts based on the quality of the user's test case. The HMIS LA may use their discretion to require new users to repeat user training. If a new user fails to successfully complete the test case requirements for data entry after repeated attempts, the HMIS LA 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 ND HMIS user license, in consultation with the ND CoC.

    c. 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.

    d. Regarding 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 ND CoC, the HMIS LA will host a link to those requirements. The HMIS LA will provide the HMIS specific workflow and report trainings.

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

2. Ongoing User Training Requirements

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

    b. All users are required to attend at one general HMIS training annually. The new user training course will count as the 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.

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

d. The HMIS LA 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.

D. HMIS User Levels

HMIS User Roles are listed on the HMIS LA website. HMIS User Roles:

1. 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.
2. 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.
3. 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.
4. 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.
5. 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.
6. 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.
7. 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.

8. Case Manager III: This role has the same actions available as the Case Manager II with the added ability to see project data for all providers on their provider tree, like an Agency Administrator.
9. Agency Administrator: Users may access all ServicePoint screens and modules. Agency Administrators can reset the passwords of users at their agency. Agency Administrators can add/remove users and edit agency and program data for all providers on their provider tree.
10. Executive Director: Users have the same access rights as an Agency Administrator but rank above the Agency Administrator.
11. 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.
12. 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.
13. System Administrator II: There are no system restrictions for System Administrator II users. They have full HMIS access. This level of access is limited to the HMIS LA for the purposes of administering and managing HMIS.

E. HMIS Vendor Requirements

1. Physical Security: Access to the areas containing HMIS equipment, data, and software will be secured. HMIS vendor staff will only access these areas to perform functions necessary to complete their job.
2. Firewall Protection: The HMIS vendor will secure the perimeter of its network using technology from firewall vendors. HMIS vendor staff monitor firewall logs to determine unusual patterns and possible system vulnerabilities.
3. User Authentication: HMIS vendor staff may only access HMIS with a valid username and password combination that is encrypted via SSL for internet transmission to prevent theft. For added security, the session key is automatically scrambled and re-established in the background at regular intervals.
4. Application Security: HMIS vendor staff will be assigned a system access level that restricts their access to appropriate data.
5. 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.
6. Technical Support: The HMIS vendor will assist the HMIS LA to resolve software problems, make necessary modifications for special programming, and will explain system functionality to the HMIS LA.
7. Technical Performance: The HMIS vendor maintains the system, including backup, data retrieval, and server functionality/operation. Upgrades to the system software will be continuously developed and implemented.

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

F. Minimum Technical Standards

1. Minimum Computer Requirements

   a. A PC with a 2 Gigahertz or higher processor, 40GB hard drive, 512 MB RAM and Microsoft Windows 7, 8, or 10.

   b. The most recent version of Firefox, Google Chrome, or Safari. No additional plug-in is required.

   c. It is recommended that the internet 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."

   d. A broadband Internet connection or LAN connection. Dial-up modem connections are not sufficient.

   e. Virus protection updates.

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

2. Additional Recommendations

   a. Memory: Windows 7, 8, or 10: 4 Gig recommended (2 Gig minimum)

   b. Monitor: Screen Display: 1024x768 (VGA) or higher; 1280x768 strongly advised

   c. Processor: A Dual-Core processor is recommended.

G. HMIS License Fees: Each July, the HMIS LA will invoice agencies for their HMIS licenses. Agencies will be invoiced based on the number of licenses allocated to them in the system at a cost of $290 per license.

H. HMIS Operating Policies Violation

1. HMIS users and Agencies must abide by all HMIS operational policies and procedures found in the HMIS Policies and Procedures manual, the ND HMIS User Policy Code of Ethics and Responsibility Statement, and the ND Agency Agreement. Repercussions for any violation will be assessed in a tiered manner. Each user or 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 policies and procedures as it relates to corrective action.

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

b. Second Violation: the user and the Agency will be notified of the violation in writing by the HMIS LA. The user's license will be suspended for 30 days. The user and/or 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 Agency notifies the HMIS LA of the action taken to remedy the violation. The HMIS LA will provide necessary training to the user and/or Agency to ensure the violation does not continue. The HMIS LA will notify the ND CoC Board of the violation during the next scheduled Board meeting following the violation.

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

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

3. Notifying the HMIS LA of a Violation: It is the responsibility of each Designated Agency HMIS Contact and general user to notify the HMIS LA when they suspect that a user or Agency has violated any HMIS operational agreement, policy, or procedure. A complaint about the potential violation must include the user and 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 LA via the HMIS LA's Help Desk email. The name of the person making the complaint will not be released from the HMIS LA if the individual wishes to remain anonymous.

4. Violations of Local, State, or Federal Law: Any Agency or user violation of local, state, or federal law will immediately be subject to the consequences listed under the Third Violation above.

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

III. Privacy and Security

The importance of the integrity and security of HMIS cannot be overstated. Given this importance, HMIS must be administered and operated under high standards of data privacy and security. The HMIS LA and Agencies are jointly responsible for ensuring that HMIS data processing capabilities, including 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 Agency must adhere, the Agency must contact ICA to collaboratively update the applicable policies for the Agency to accurately reflect the additional protections.

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

1. 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.
2. Not Shared Data: 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 (unless signed by a legal guardian), or legal services must enter not shared data. Individual client records can be not shared at the client's request.
3. Procedures for transmission and storage of data
    a. 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.
    b. 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.
    c. 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.
    d. All public data must be classified as aggregated public and unpublished restricted access data.
        - Aggregated Public Data: Information published according to the "Data Reporting Parameters and Guidelines" (HMIS Policies and Procedures Section III.B).
        - 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.
4. Procedures for Transmission and Storage of Data

a. Aggregated Public Data: Security controls are not required.

b. Unpublished Restricted Access Data

- 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.
- 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.

B. 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.

1. No identified client data may be released without the informed consent of the client, unless otherwise specified by ND state and federal confidentiality laws. All requests for such information must be addressed to the owner/Agency where the data was collected.
2. 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 of that program.
3. There will be full access to aggregate data included in published reports.
4. Reports of aggregate data may be made directly available to the public.
5. The parameters of the aggregated data, that is, where the data comes from and what it includes will be presented with each report.
6. Data will be provided to agencies requesting reports on a case-by-case basis.
7. 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.
8. ICA reserves the right to deny any request for aggregated data, in consultation with the ND CoC. Final decisions will be made by the HMIS director and ND CoC coordinator.

C. Release of Data for Grant Funders: Entities providing funding to agencies or programs required to use HMIS will not have automatic access to HMIS. Access to HMIS will only be granted by the HMIS LA 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.

D. Baseline Privacy Policy

1. Collection of Personal Information

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

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

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

c. Personal information is collected with the knowledge and consent of clients. It is assumed that client's 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.

d. 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.

e. Personal information may also be collected from:

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

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

2. 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 reason not described here.

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

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

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

   c. For academic research conducted by an individual or institution that has a formal relationship with the HMIS LA and is approved by the ND CoC. The research must be conducted by an individual employed by or affiliated with the organization or institution. All research projects must be conducted under the 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 agrees to comply with all the terms and conditions of the written research agreement.
- Be substituted, when appropriate, by the Institutional Review Board, Privacy Board, or other applicable human subjects' protection institution approval.

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

e. 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 reasonably able to prevent or lessen the threat, including the target of the threat.

f. 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 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.

g. 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. It is the responsibility of the HMIS LA or Agency to provide the information requested.
   - If the law enforcement official makes a written request for personal information including that which constitutes evidence of criminal conduct that occurred at the agency where the client receives services. The written request must meet the following requirements:

- Be signed by a supervisory official of the law enforcement agency seeking the personal information;
- State how the information is relevant and material to a legitimate law enforcement investigation;
- Identify the person for information sought;
- Be specific and limited in scope to the purpose for which the information is sought; and
- It is the responsibility of the HMIS LA or Agency to provide the information requested.

- If the official is an authorized federal official seeking personal information for the provision of protective services to the President or other persons authorized by 18 U.S.C 3056 or to a foreign head of state or other persons authorized by 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.

h. 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.

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

3. Inspection and Correction of Personal Information

a. 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.

b. 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.

c. 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.

d. 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.

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

4. Limits on Collection of Personal Information

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

   b. Client files not used in seven years may be made inactive in HMIS. The HMIS LA 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.

5. Limits on Partner Agency Use of HMIS Client Information

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

   b. Youth providers serving unaccompanied minors under the age of 18 must maintain HMIS files that are not shared. Unaccompanied youth under the age of 18 may not provide either written or verbal consent to the release of their personally identifying information in HMIS. If the agency receives consent from the unaccompanied youth's legal guardian, data about the youth can be shared in HMIS; otherwise, it will be entered in HMIS unshared.

6. Complaints about Accountability

   a. 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 HMIS LA and the HMIS LA's executive director. If there is no resolution, the ND CoC Board will oversee the final arbitration. All other complaints will follow the agency's grievance procedure as outlined in the Agency's handbook.

   b. 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 this privacy notice.

E. 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 into or provide data for HMIS, as they are legally prohibited from participating in HMIS. Victim service providers that are recipients of funds requiring participation in HMIS, but are prohibited from entering data in HMIS, must use a comparable database to enter client information. A comparable database is a database that can use collected client-level data over time and generate unduplicated aggregated reports based on the client information entered in the

database. The reports generated by a comparable database must be accurate and provide the same information as the reports generated by HMIS.

F. User Conflict of Interest: Users who are also clients with files in HMIS are prohibited from entering or editing information in their own file. All users are also prohibited from entering or editing information in the files of immediate family members. All users must sign the ND 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 HMIS LA may run the audit trail report to determine if there has been a violation of the conflict of interest agreement.

G. Privacy and Security Training for Users: All users must receive privacy and security training prior to being given access to HMIS. Privacy and security training is covered during the new user training for all new users. All users must receive on-going annual training on privacy and security from the HMIS LA.

H. Violation of Security Procedures

1. 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.
2. 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 HMIS LA and placed in the client's file at the Agency that originated the client's record.
3. 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 HMIS LA. All sanctions may be appealed to the ND CoC Board.

I. 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 HMIS LA. The HMIS LA will use the HMIS user audit trail report to determine the extent of the breach of security.

J. Disaster Recovery Plan

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

1. Database tape backups occur nightly.
2. Tape backups are stored offsite.
3. Seven-day backup history is stored locally on instantly accessible Raid 10 storage.
4. One-month backup history is stored offsite.

5. Access to WellSky's emergency line to provide assistance related to "outages" or "downtime" 24 hours a day.
6. Data is backed up locally on instantly accessible disk storage every 24 hours.
7. 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.
8. Backups of the application site are near-instantaneous (no files older than five minutes).
9. The database is replicated nightly at an offsite location in case of a primary data center failure.
10. Priority level response (ensures downtime will not exceed four hours).

IV. Data Requirements

A. Minimum Data Collection Standard

1. 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 the HMIS LA. The required data elements depend on the program.
2. The Designated Agency HMIS Contact must identify the assessments and data element requirements for each project. The HMIS LA will consult with the Designated Agency HMIS Contact to properly set up each project in HMIS.
3. Guidelines clearly articulating the minimum expectations for data entry for all projects entering data in HMIS will be sent to the Designated Agency HMIS Contacts and posted on the HMIS LA's website. Designated Agency HMIS Contacts must ensure that the minimum data elements are fulfilled for every project.

B. Provider Naming Convention: All providers within HMIS must be named so they accurately reflect the type of service carried out by the corresponding Agency project.

C. 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 CoC 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 the persons at-risk of and experiencing homelessness and the projects that serve them. Specifically, the goal is to record the most complete, accurate, consistent, and timely information in order to draw reasonable conclusions about the extent of homelessness and the impact on the homeless services system. To that end, the ND CoC will collectively assess the quality of our data by examining characteristics such as timeliness, completeness, and accuracy.

D. Data Imports: While HMIS databases are required to have the capacity to accept data imports, the CoC reserves the right not to allow data imports into HMIS. Allowing data imports will impact data integrity and increase the likelihood of duplication of client files in the system.

E. HMIS Data Protections: It is the responsibility of the HMIS LA to maintain the HMIS, including protecting the data contained in HMIS. In the case where the HMIS LA is made aware through data contained in HMIS that Agency program funds were used for an ineligible service, the HMIS LA will notify the Agency about the misuse of funds. If the Agency fails to rectify the misuse of funds in a timely fashion, the HMIS LA will notify the appropriate funding body.

V. Glossary

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

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

C. Confidential Data: contains personal identifying information.

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

E. Homeless Management Information System (HMIS): 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.

F. HMIS Lead Agency: the entity designated by the CoC in accordance with the CoC Interim Rule to operate the CoC's HMIS on its behalf.

G. North Dakota Continuum of Care Board: the group of ND CoC members who are responsible for approving and implementing the HMIS Policies and Procedures, and for working to make improvements to North Dakota's HMIS.

H. HMIS License Fee: the annual fee paid by Agencies to allow each HMIS user at their agency continued access to the database.

I. HMIS User Level: HMIS users are assigned a specific user level that limits the data the user can access in the database.

J. HMIS Vendor: North Dakota's HMIS software vendor is WellSky Community Services. The HMIS vendor designs the HMIS and provides ongoing support to the HMIS LA.

K. Universal Data Elements: a minimum set of questions that must be completed for each client to provide data for use in aggregate analysis.

L. Open Data: does not contain personal identifying information.

M. Partner Agencies: the homeless service agencies that use HMIS.

N. Program Specific Data Elements: to meet the statutory and regulatory requirements of federally funded programs using HMIS, elements are required for different funding sources. The Program Specific Data Elements are elements required by at least one of the HMIS Federal Partner programs.

O. System Administrator(s): staff at the HMIS LA who are responsible for overseeing HMIS users and use in ND. The System Administrator(s) allow users HMIS access and provide training, ensure user compliance with HMIS policies and procedures, and make policy recommendations to the ND CoC Board.

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

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

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

VI. HMIS Policies and Procedures

HMIS Policies and Procedures include:

A. Data Dictionary and Data Manual (Appendix 1)

B. Data Quality Management Plan

VIII. Acknowledgement of Receipt of ND HMIS Policies and Procedures, Privacy Notice, and Data Quality Management Plan

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

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

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

_____ _____

Signature Date

_____

Print Name

_____

Agency

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 LA, HMIS System Administrator(s), and users. The companion document to the HMIS Data Standards Manual is the HMIS Data Dictionary.

The HMIS Data Dictionary is designed for HMIS vendors, HMIS LA, and HMIS System Administrator(s) to understand all 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 databases must be able to collect all 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 here.