North Dakota-500
Statewide Continuum of Care

Privacy Plan

CoC Board Approval: July 20, 2020
CoC Membership Approval: August 5, 2020

Next Review: July 2021

The importance of the integrity and security of the Homeless Management Information System (HMIS) cannot be overstated. Given this importance, HMIS must be administered and operated under high standards of data privacy and security. The HMIS Lead 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.

I. 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.

A. 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 for most projects.

B. 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 (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.

C. Procedures for transmission and storage of data

1. 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.
2. 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.
3. Whenever confidential data is accessed:
    a. 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.
    b. Hard copies shall not be left out in the open or unattended.
    c. Electronic copies shall be stored only where the employee can access the data.
    d. Electronic copies shall be stored where a password is required to access the data if on shared server space.

4. All public data must be classified as aggregated public and unpublished restricted access data.
    a. Aggregated Public Data: Information published according to the “Reporting Parameters and Guidelines” (HMIS Policies and Procedures Section III.B).
    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.

D. Procedures for Transmission and Storage of Data
    1. Aggregated Public Data: Security controls are not required.
    2. Unpublished Restricted Access Data:
        a. 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.
        b. 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.

II. Data Reporting Parameters and Guidelines

A. All open data will be handled according to the following classifications:
    1. Public Data: Data that does not contain personally identifiable information (PII).
    2. Internal Data: Confidential data that contains PII at the organization or project level.
    3. Restricted Data: Confidential data that contains PII at the multi-organization or system level.

B. 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 North Dakota 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 CoC. Final decisions will be made by the HMIS Director and CoC Coordinator.

III. Release of Data for Grant Funders

Entities providing funding to agencies or programs required to use HMIS will not have automatic access to HMIS. Access to HMIS will only be granted by the HMIS Lead 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.

IV. Baseline Privacy Policy

A. Collection of Personal Information

1. 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:
    a. To provide or coordinate services for clients.
    b. To find programs that may provide additional client assistance.
    c. To comply with government and grant reporting obligations.
    d. 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.
2. Only lawful and fair means are used to collect personal information.
3. 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.
4. 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.
5. Personal information may also be collected from:
    a. Additional individuals seeking services with a client.
    b. Other agencies that provide services and participate in HMIS.
6. Upon request, clients must be able to access the *Use and Disclosure of Personal Information* policy found below.

B. 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:

1. To carry out administrative functions such as legal audits, personnel oversight, and management functions.
2. For research and statistical purposes. Personal information released for research and statistical purposes will be anonymous.
3. For academic research conducted by an individual or institution that has a formal relationship with the HMIS Lead and is approved by the 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:
    a. Establish rules and limitations for processing personal information and providing security for personal information in the course of the research.
    b. Provide for the return or proper disposal of all personal information at the conclusion of the research.
    c. Restrict additional use or disclosure of personal information, except where required by law.
    d. Require that the recipient of the personal information formally agrees to comply with all the terms and conditions of the written research agreement.
    e. Be substituted, when appropriate, by Institutional Review Board, Privacy Board, or other applicable human subjects' protection institution approval.
4. When required by law, personal information will be released to the extent that use or disclosure complies with the requirements of the law.
5. To avert a serious threat to health or safety if:
    a. 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
    b. The use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat.
6. 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:
    a. It is believed that informing the individual would place the individual at risk of serious harm, or
    b. 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.

7. For a law enforcement purpose (if consistent with applicable law and standards of ethical judgement) under any of these circumstances:
    a. 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 Lead or Agency to provide the information requested.
    b. 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 Lead or Agency to provide the information requested.
    c. 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.
8. 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.
9. To comply with government reporting obligations for homeless management information systems and for oversight of compliance with homeless management information system requirements.

C. Inspection and Correction of Personal Information

1. 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.
2. 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.

3. A request to inspect or copy one's personal information may be denied if:
    a. The information was compiled in reasonable anticipation of litigation or comparable proceedings;
    b. The information was obtained under a promise or confidentiality and if the disclosure would reveal the source of the information; or
    c. The life or physical safety of any individual would be reasonably endangered by disclosure of the personal information.
4. 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.
5. Requests for inspection and access or personal information correction may be denied if they are made in a repeated and/or harassing manner.

D. Limits on Collection of Personal Information
    1. Only personal information relevant for the purpose(s) for which it will be used will be collected. Personal information must be accurate and complete.
    2. Client files not used in seven years may be made inactive in HMIS. The HMIS Lead 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.

E. Limits on Partner Agency Use of HMIS Client Information
    1. The North Dakota 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.
    2. 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.

F. Complaints about Accountability
    1. 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 Lead and the HMIS Lead's executive director. If there is no resolution, the CoC Board will oversee the final arbitration. All other complaints will follow the agency's grievance procedure as outlined in the Agency's handbook.

2. 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.

V. 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.

VI. 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 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 HMIS Lead may run the audit trail report to determine if there has been a violation of the conflict of interest agreement.

VII. 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 Lead.

VIII. Violation of Security Procedures

A. 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.

B. 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 Lead and placed in the client's file at the Agency that originated the client's record.

C. 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 Lead. All sanctions may be appealed to the CoC Board.

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

X. Disaster Recovery Plan

A. WellSky Community Services Disaster Recovery Plan

B. 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 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).