CENTER ON CHILDREN, FAMILIES, AND THE LAW

Nebraska BOS and Lincoln CoCs HMIS Security, Privacy, and Data Quality Plan

This plan is intended to meet the requirements of 24 CFR 578.7(b)(3) for the Balance of State and Lincoln CoCs. The plan works in conjunction with the Nebraska Management Information System Policies and Standard Operating Procedures Manual and HUD regulation and guidance such as 24 CFR Part 578, the 2004 HMIS Data and Technical Standards Final Notice (69 Fed. Reg. 45888 (July 30, 2004/Notices)), HMIS Data Standards (Published 2024), Coordinated Entry Management and Data Guide (Published 2018), and Proposed HMIS Requirements (76 Fed. Reg. 76917 (December 9, 2011))

Operation of HMIS involves partnerships between the Balance of State CoC, Lincoln CoC, HMIS Lead, and Participating Agencies.

Nebraska BOS and Lincoln CoCs HMIS Security, Privacy, and Data Quality Plan

The Nebraska Homeless Management Information System (HMIS) is a locally administered electronic data collection system that stores longitudinal person-level information about the individuals and families who access homeless and other human services in a community.

By streamlining and consolidating recordkeeping requirements, HMIS allows us to provide an accurate and effective presentation of homelessness on program, agency, continuum, and statewide levels. The reports generated using HMIS data serve as the foundation on which the Balance of State and Lincoln CoCs can plan and prepare to prevent, reduce, and eliminate homelessness.

Because Balance of State and Lincoln receive Housing and Urban Development (HUD) Continuum of Care (CoC) funding, they must implement and maintain an HMIS to capture standardized data about all persons accessing the homeless assistance system. Furthermore, elements of HUD's annual CoC funding completion are related directly to a CoC's progress in ending homelessness which is supported by data from the HMIS.

In 2004, HUD published in the Federal Register the HMIS Data and Technical Standards which define the requirements for data collection, privacy safeguards, and security controls for all local HMIS implementations (69 Fed. Reg. 45888 (July 30, 2004/Notices)). In 2023 HUD published changes in the HMIS Data Standards Version 1.5 released in May 2023 and updated in February 2024 (https://www.hudexchange.info/resource/3824/hmis-data-dictionary/).

The intent of this plan is to set forth policies and procedures for the Balance of State CoC, Lincoln CoC, and all Participating Agencies to comply with the HUD regulations and guidance regarding safeguarding the privacy of clients, the security of their personal information, and the quality of the data entered in the HMIS.:

- HMIS Technical Standards (Federal Register Vol. 76, No. 237 §580.33)
- HMIS Security Standards (Federal Register Vol. 76, No. 237 §580.35)

All persons using NMIS/HMIS are expected to read, understand, and adhere to:

- The 2024 HMIS Data Standards Version 1.5; February 2024
- HUD Homeless Management Information Systems (HMIS); Data and Technical Standards Final Notice; 69 FR 146 (pp. 45888-45934)
- Nebraska Management Information System Policies and Standard Operating Procedures Manual

Contents

ACRONYMS & DEFINITION OF TERMS

This list includes a list of terms used throughout this document.

Agency Administrator Each Participating Agency appoints an Agency Administrator to act as the contact person for the System Administrators and to manage the operation of the HMIS within the agency and its projects.

CAN Community Action of Nebraska is an NMIS Member organization. CAN is the statewide agency comprising the nine local Community Action agencies (CAAs) in Nebraska. CAN acts as the system administrator for service-only projects at Community Action agencies and SSVF funded projects.

CCFL UNL-Center on Children, Families and the Law is an NMIS Member organization and is the HMIS Lead for the Balance of State CoC and Lincoln CoC. CCFL acts as the system administrator for all housing projects and all non-Community Action service-only projects in the Balance of State and Lincoln CoCs.

Client An individual about whom a Participating Agency collects or maintains protected personal information (1) because the individual is receiving, has received, may receive, or has inquired about services from agency or (2) in order to identify services, needs, or to plan or develop appropriate services within the CoC.

CoC Continuum of Care means the group composed of representatives from organizations including nonprofit homeless providers, victim service providers, faith-based organizations, governments, businesses, advocates, public housing agencies, school districts, social service providers, mental health agencies, hospitals, universities, affordable housing developers, law enforcement, organizations that serve veterans, and homeless and formerly homeless persons organized to carry out the responsibilities of a Continuum of Care established under 24 CFR part 578.

Data:

Aggregated Public Data De-identified data available to the public.
Locked Data Data entered by one Participating Agency that is not visible to other agencies using HMIS.
Open Data Data that is visible to all Participating Agencies using HMIS.

Data Recipient A person who obtains PPI from an HMIS Lead or from a Participating Agency for research or other purpose not directly related to the operation of the HMIS, CoC, HMIS Lead, or Participating Agency.

End User Any system user who has an active HMIS software license.

HMIS Homeless Management Information System means the information system designated by Continuums of Care to comply with the requirements of HUD and used to record, analyze, and transmit client and activity data in regard to the provision of shelter, housing, and services to individuals and families who are homeless or at risk of homelessness.

HMIS Lead means an entity designated by the Continuum of Care in accordance with 24 CFR 578.7(b)(2) to operate the Continuum's HMIS on its behalf. CCFL is the HMIS Lead for the Balance of State and Lincoln CoCs.

HMIS vendor means a contractor who provides materials or services for the operation of an HMIS. An HMIS vendor includes an HMIS software provider, web server host, and data warehouse provider, as well as a provider of other information technology or support.

HUD means the Department of Housing and Urban Development.

HMIS Committee is a group composed of representatives from interested Participating Agencies who assist in making decisions regarding the HMIS system, HMIS policies and procedures, and any concerns that arise regarding HMIS.

HMIS Participation Agreement is a written agreement between the HMIS Lead and each Participating Agency that details the responsibilities of each party regarding participation in the HMIS.

MOU Memorandum of Understanding

Participating Agency Any organization, including its employees, volunteers, and contractors, that accesses HMIS and records, uses or processes Protected Personal Information. In some HUD materials, this is also referred to as a Contributing HMIS Organization (CHO).

Privacy is the control over the extent, timing, and circumstances of sharing oneself (physically, behaviorally, or intellectually) with others. Privacy consists of ensuring specific measures are in place when dealing with personal information and includes directives on when it is collected, how that information is used, and how that information is shared with others.

Privacy Standards apply to all Agencies and Programs that record, use, or process Protected Personal Information (PPI) within the HMIS, regardless of funding source.

PPI Protected Personal Information means any information about a client that (1) identifies a specific individual, (2) can be manipulated so that identification is possible, and (3) can be linked with other available information to identify a specific individual. This can include: name, SSN, program Entry/Exit, zip code of last permanent address, system/program ID, and program type.

Research A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to general knowledge.

ROI Release of Information.

System Administrator (SA) Staff at the HMIS Lead or other NMIS Member organization who are responsible for overseeing HMIS users and system use/access

within Nebraska. The System Administrators allow End User HMIS access, provide End User training, ensure user compliance with HMIS policies and procedures, and make policy recommendations to the NMIS Board.

UDE Universal Data Elements are data elements required to be collected by all projects participating in the HMIS and include HUD data elements 3.01-3.07 and Client Location.

UPSE Universal Project Stay Elements are data elements required to be collected by all housing projects participating in the HMIS and include HUD data elements 3.08-3.917.

Security and Privacy Plan

This plan is designed to establish security and privacy standards for participating agencies within the Balance of State CoC and Lincoln CoC. This plan is designed to be consistent with and aid in implementing the NMIS policies around the security and privacy of the HMIS. The following requirements and recommendations are informed by the Security Standards as defined in the Proposed HMIS Requirements (76 Fed. Reg. 76917 (December 9, 2011)). This plan sets the expectations for both the community and the end users to make sure they are taking appropriate measures to keep consumer information safe and secure.

HMIS Security Standards §580.35(a) Security standards, as provided in this section, are directed to ensure the confidentiality, integrity, and availability of all HMIS information; protect against any reasonably anticipated threats or hazards to security; and ensure compliance by end users. Written policies and procedures must comply with all applicable Federal law and regulations, and applicable state or local governmental requirements.

Security Plan §580.35(c)(1) All HMIS Leads must develop a HMIS security plan, which meets the minimum requirements for a security plan as established by HUD in notice, and which must be approved by the Continuum of Care.

Commitment to Privacy

NMIS is committed to preserving the privacy of clients whose personal identifying information is entered into the HMIS. Clients' personal information will not be shared without express consent from the clients. Participating agencies will take all steps necessary to safeguard the confidentiality of their clients' personal information both in and out of the HMIS.

Privacy Notice and Privacy Policy

Participating Agencies are required to have a privacy policy complying with NMIS policy 601. Participating Agencies must post the NMIS Consumer Notice (Appendix E of the NMIS SOP Manual) in all client intake areas and high-traffic areas. The NMIS Consumer Notice can be customized to reflect additional aspects of the Participating Agency's privacy policy.

Consent to Share Information

NMIS is an open system with statewide data sharing to facilitate coordination of services between Participating Agencies. Prior to entering any client information into the HMIS, Participating Agencies must request informed consent from every client to share their information through NMIS. Clients may choose not to share their information in NMIS, and Participating Agencies may not limit or deny services based on a client's refusal to allow their information to be shared. Participating Agencies must inform each client of the agency's participation in NMIS and what information will be

shared, with whom it is being shared, and for what purposes. Each adult must have the opportunity to consent or deny consent for their information to be shared for themselves. Heads of household cannot consent to information sharing on behalf of other adult household members. Only a parent or guardian can consent to the sharing of a minor's information in NMIS.

NMIS Client Release of Information

Each client must have the opportunity to sign a paper or electronic copy of the NMIS Client Release of Information (Appendix F to the NMIS SOP Manual). Verbal consent is allowed for electronic or telephone assessment. Participating Agencies are expected to present clients who participate in in-person services with a paper ROI upon receiving those services. The NMIS ROI is a system-wide release. Once a client has consented to the sharing of their information in NMIS, all Participating Agencies may rely on that consent to enter and share information relating to that client. By default, the NMIS ROI ends one year from the date of the consent. Specific programs who request ROIs for longer than one year must clearly identify the expiration date of the ROI on the face of the document before the client gives the consent.

Refusing Consent to Share Information

Clients may choose not to share their information in NMIS, and Participating Agencies may not limit or deny services based on a client's refusal to allow their information to be shared. Client consent is required to share information in NMIS, but consent is not required to enter and store client information in NMIS. If a client refuses consent to share their information, the agency will take into consideration whether this is a new client record or an existing client record. If the client already has a profile in NMIS, the Participating Agency will use that profile and will lock their program enrollment to that agency. If this is a new client record, the Participating Agency will create the client profile in NMIS and lock the client profile to that agency

Revoking Consent to Share Information

A client has the right to revoke their consent to share information in NMIS using the NMIS Revocation of Consent (Appendix G to the NMIS SOP Manual). The client revokes consent to share information on an agency-by-agency basis. Client information that has already been shared in NMIS under a valid ROI will not be removed from the NMIS and will remain shared. New client information will not be shared by the agency collecting the revocation.

HMIS Lead (CCFL)

The HMIS Lead shall uphold the following duties and responsibilities:

- Adherence to the Security, Privacy and Data Quality Plan
- Review the Security, Privacy and Data Quality Plan annually and at the time of any change to the Security management process of any HMIS data or technical requirements issued by HUD. When changes are required to the HMIS Privacy,

Security and Data Quality Plan, the HMIS Lead will work with the NMIS System Administrators for review, modification and approval.
- Respond to any security questions, requests, or security breaches to the HMIS and communication of security-related HMIS information to Participating Agencies.

System Administrators (CAN, CCFL)

System Administrators shall uphold the roles and requirements recited in the NMIS Policy and Standard Operating Procedures manual, including:

- Adherence to the Security, Privacy, and Data Quality Plan
- Provide training to individual HMIS Users
- Support project reporting requirements at the CHO and CoC levels, working with other System Administrators prior to preparing reports that include data from more than one CoC or CAN.

Participating Agencies

Each Participating Agency is responsible to uphold the following duties/responsibilities:

- Adherence to the Security, Privacy and Data Quality Plan
- Ensure the confidentiality, integrity, and availability of all HMIS information.
- Protect against any reasonable anticipated threats to security.
- Ensure compliance by End Users
- Participate in security training offered by the HMIS Lead

HMIS Security Requirements

HMIS Security Officer

The HMIS Lead must designate one staff member as the HMIS Security Officer. Each Participating Agency must also designate an internal HMIS Security Officer that will work directly with the HMIS Lead to be responsible for ensuring compliance with applicable security standards within the agency. The Participating Agency Security Officer does not need to be the Agency Administrator, but they must be an employee of the agency and an End User with access to the system. For any agency without employees, the HMIS Security Officer must be the President, Chair, or other top-level representative responsible for the agency.

Workforce Security

The HMIS Lead must conduct a criminal background check on its HMIS Security Officer. Participating Agencies are strongly encouraged to perform background checks to ensure the safe handling of client data, especially on their designated Agency Administrator-level access or greater. Criminal Background checks must include local and state records; Participating Agencies are strongly encouraged to include federal records as well but are not required to do so.

Security and Privacy Awareness Training and Follow-up

System Administrators shall ensure that all End Users receive security and privacy awareness training prior to being given access to the HMIS. This training can be conducted either live (in-person or virtually) or via on-demand module. The HMIS Lead will conduct security and privacy awareness training on an annual basis, which will be required for all End Users and Security Officers. This training will cover relevant statutory and regulatory requirements, local policies, and best practices for HMIS Privacy and Security. If an End User or Security Officer does not attend the required annual training, their access to HMIS will be restricted until they attend training.

Reporting Security Incidents

Users must report all unauthorized access of HMIS and unauthorized attempted access of HMIS. This includes theft of usernames and passwords. Security incidents must be reported to a System Administrator. The System Administrators will use available reports and system tools to determine the extent of the breach of security. The HMIS Lead must abide by the following policy and chain of communication for reporting and responding to security incidents.

Chain of Reporting:

End Users should report issues first to their Participating Agency's designated Security Officer within one business day. Security Officers should report the issue jointly to the Participating Agency Executive Director and the HMIS Lead within one business day. Each Participating Agency is responsible for reporting any security incidents involving the real or potential intrusion of the HMIS system. End Users must report any incident in which unauthorized use or disclosure of Protected Personal Information (PPI) has occurred and any incident in which PPI may have been used in a manner inconsistent with the Nebraska HMIS Security, Privacy, and Data Quality Plan. The HMIS Software maintains an accessible audit trail that allows any System Administrator to monitor user activity and examine data access for specified users.

Users who are clients or have close relationships with clients in HMIS

End Users must disclose any potential conflict of interest to their Agency Administrator or Executive Director. End Users will be prohibited from making changes to the information in their own file or the files of their immediate family members or their friends/acquaintances. If an End User is suspected of violating this prohibition, the System Administrators will run an audit report to determine if there was an infraction. Infractions will be reported to the Agency Administrator and the End User's access will be suspended. Disciplinary actions are the responsibility of the end user agency. Access will only be restored at the request of the agency Executive Director or Chief Executive Officer, as applicable.

Current guests in shelter or facility-based housing may not have access to NMIS as volunteers or employees in order to preserve confidentiality for other clients.

Participating Agencies who wish to hire or use as a volunteer any former client of one of that Participating Agency's programs are encouraged to establish a minimum 90-day probationary period before access to NMIS is granted. Participating Agencies who wish to hire or use as a volunteer any former client of any Participating Agency's shelter or facility-based housing may grant access to NMIS at their discretion.

Security of Content in Reports

General extracts (Excel, CSV, or any other format) of data from the HMIS and any reports generated by any Participating Agency may be made publicly available and/or shared with other agencies and organizations provided the report contains no Protected Personal Information. Any report that includes a client's name, date of birth, and/or social security number or any combination of data that, taken together, could constitute PPI may not be shared outside your agency.

Disaster Recovery Plan

The Disaster Recovery Plan for HMIS is the responsibility of our HMIS Vendor, Bitfocus, which hosts and houses the data on remote servers. The vendor, Bitfocus, will perform regular scheduled backups of the system to prevent loss of data.

In the event of a disaster involving substantial loss of data or system downtime, the HMIS Lead will contact Participating Agency Security Officers by phone or email within one business day to inform them of the expected scale and duration of the loss or downtime.

Non-HUD Funded Participating Agencies

Participating Agencies that are not funded by HUD programs but utilize HMIS must comply with the same policies and procedures as Agencies that are funded by HUD. Failure to comply may result in termination of the Agency's access to HMIS.

Security Reviews

All Participating Agencies are encouraged to perform regular security reviews, which will include at minimum the completion of a Security and Privacy Checklist (See Appendix B). Agency Administrators will work with the Participating Agency Security Officer to schedule a review and will assist with performing the review. The results of the review must be returned to the HMIS Security Officer via Fax or Email the same day it is completed. Any items needing to be fixed must be fixed within 10 working days.

The HMIS Lead may require any Participating Agency to undergo a random Security Review once in a calendar year; however, if a Participating Agency has already submitted a security review during that calendar year that previous review will satisfy the HMIS Lead's request.

The HMIS Lead may require any Participating Agency to undergo additional security reviews at any time in response to frequent, repetitive, or serious security or privacy issues identified by the HMIS Lead.

Contracts and other arrangements

The HMIS Lead must retain copies of all contracts and agreements executed as part of the administration and management of HMIS or required to comply with HUD policies.

Physical and Technical Safeguards

Physical Safeguards §580.35(e). The HMIS Lead must implement physical measures, policies, and procedures to protect the HMIS.

Technical safeguards §580.35(f). The HMIS Lead must implement security standards establishing the technology that protects and controls access to protected electronic HMIS information and outline the policy and procedures for its use.

Each Participating Agency must apply physical and technical system security provisions to all the systems where PPI is entered, transmitted, used, or stored, including but not limited to a Participating Agency's networks, desktops, laptops, mini-computers, mobile devices, mainframes, and servers. The software used for HMIS is accessed over the internet; a broadband internet connection is necessary.

User Authentication: NMIS Passwords

The NMIS software requires a user authentication system consisting of a username and a password. Every licensed end user is required to have a unique User ID and password, account sharing IS NOT allowed under any circumstances.

Using default passwords on initial entry into the HMIS application is allowed so long as the application requires the default password to be changed on first use. Information specifically pertaining to end user access (e.g., username and password) may NOT be stored or displayed in any publicly accessible location. Individual end users must not be able to log on to the HMIS at more than one location at a time.

- Creation: Passwords are automatically generated from the system when a user is created. The System Administrator will communicate the one-time password to the user.
- Use: The end user will be required to change the password the first time they log into the system. The password must be between eight and sixteen characters and must contain characters from the following four categories: uppercase characters (A through Z), lowercase characters (a through z), numbers (0 through 9), and non-alphanumeric characters (!@#$%()^&*). Passwords cannot contain spaces, the word 'clarity,' the word 'NMIS,' the user's first name, last name, or username, 'ABC' or '123,' or the same character more than twice consecutively. Passwords

must not be able to be guessed easily. Passwords are the individual's responsibility and end users CANNOT share passwords.

- Storage: Passwords are to be stored securely and must be inaccessible to other people. End Users are not to electronically store passwords on a computer for easier log-on.
    - End Users should memorize their NMIS passwords to avoid writing them down.
    - Participating Agencies will not, under any circumstances, demand that an End User turn over their password.
- Expiration: HMIS passwords expire every 120 days. End users may not use the same password consecutively. Passwords cannot be re-used until three password selections have expired.
- Unsuccessful login: If an end user unsuccessfully attempts to log on three (3) times, the end user's account will be locked, and access permission will be revoked rendering the end user unable to gain access until the account is unlocked. End Users must contact a System Administrator to have their account unlocked.

Device Security

A Participating Agency must secure the devices used by its End Users to access HMIS. All devices accessing HMIS must be placed in secure locations or must be attended at all times if they are in publicly accessible locations. Any devices that are not themselves used to access HMIS but are networked with devices accessing HMIS should be similarly secured. End Users should ensure that devices are positioned or held in a manner where it is difficult for others to see the contents of their screens. Participating Agencies should consider the use of privacy-protecting screens when devices are used in publicly visible locations. Printers that are used to print hard copies from HMIS must be in secure locations or must be attended to while printing.

All devices accessing HMIS must have a password-protected login for the device itself and must automatically lock after five to eight minutes of inactivity. Participating Agencies are highly encouraged to set up personalized logins for each End User who uses a device rather than setting up a generic or shared device login. End Users should always lock their devices whenever they are unattended for any amount of time.

Data Security

Participating Agencies must secure HMIS data in transmission and in storage. NMIS is a cloud-based software and does not require any data to be saved locally on the device used to access it. Participating Agencies should establish procedures to minimize the amount of HMIS data that is saved locally on devices, particularly easily movable devices like laptops, tablets, flash drives, and portable hard drives. HMIS data should never be stored on unencrypted mobile devices. Participating Agencies must also secure hard copies of HMIS data including printouts and physical forms used to gather the

information entered into HMIS. Physical files should be stored in secure locations and locked filing cabinets. Forms and documents that are scanned for upload to HMIS should be saved in secure storage locations and the scans should be deleted from local devices after being uploaded to HMIS. Internet browsers that are used to access HMIS should be set to delete temporary files and browsing history upon exit.

HMIS should never be accessed using an unsecured Wi-Fi network or unsecured internet connection. Publicly available but password-protected Wi-Fi networks such as those offered to customers in coffee shops, hotels, airports, and libraries should not be used to access HMIS unless a secure Virtual Private Network (VPN) is used to encrypt and secure the connection to HMIS. Emails containing PPI or other confidential information must be encrypted using at least 128-bit encryption. All emails sent by End Users or agency Security Officers must include a confidentiality notice (see Appendix A).

Virus Protection

A Participating Agency must protect HMIS systems from viruses by using commercially available virus protection software. Virus protection must include real-time scanning of downloaded files and emails and regular scanning of the system at least weekly. A Participating Agency must regularly update virus definitions from the software vendor. No flash drives or other portable media devices will be introduced to any device accessing HMIS without being first scanned to ensure such devices do not have any computer viruses or other malware.

Firewalls

A Participating Agency must protect HMIS systems from malicious intrusion behind a secure firewall and routinely monitor for intrusion attempts. Each individual device does not need its own firewall, as long as there is a firewall between that device and any systems, including the Internet and other computer networks, located outside of the organization. For example, a device that accesses the Internet through a modem would need its own firewall. A device that accesses the Internet through a central server or local network would NOT need a firewall as long as the server or local network has a firewall. If computers are networked with wireless connections, the network must have up to date and industry standard security and the network must be password protected.

Operating Systems and Internet Browsers

A Participating Agency must take reasonable steps to ensure that all devices accessing the HMIS are protected from compromise due to outdated software or operating systems. All devices accessing HMIS must be running a current operating system and the most up-to-date version of a current internet browser. An OS or browser that is no longer actively and regularly supported with updates from the developer is not current. All browsers should be set to automatically download and install version updates as they become available. All devices must be set to automatically download and install all security updates for the operating system, either through the OS's built-in features (e.g.,

Windows Update, macOSX Software Update) or through an update management product managed by the Participating Agency's IT provider.

Desk and/or Onsite Monitoring

HMIS Lead will monitor HMIS participation through periodic and annual desk and/or onsite security reviews to ensure implementation of the security requirements. Additionally, data in HMIS will be reviewed regularly.

A security audit checklist for the security reviews will be provided to Agencies with expectations of monitoring. The goal of the audit is to ensure that Agencies are complying with security requirements. HMIS Lead will work with agencies that receive findings to ensure they are remedied as quickly as possible for the benefit of all Agencies who utilize HMIS.

Ongoing Monitoring

Agency Administrators are encouraged to conduct regular security reviews for all devices that will access HMIS; this includes ensuring devices are protected by firewall and antivirus software as appropriate.

The Agency Security Officers are responsible for managing the selection, development, implementation, and maintenance of security measures to protect HMIS information within their agency. The Agency Security Officer will use the Compliance Certification Checklist to audit their devices in their Agency. Should the Checklist contain one or more findings, the finding will need to be resolved withing seven business days. The Agency Security Officer must turn in a copy of the Compliance Certification Checklist to the HMIS Lead after each completion.

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. A formal letter of reprimand
b. Suspension of system privileges
c. Revocation of system privileges
d. Criminal prosecution

If possible, all confirmed security violations will be communicated in writing by the HMIS Lead within 14 days. 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 and shall be reported to the appropriate funder. All sanctions may be appealed to the NMIS Board.

Sanctions for Violations

There are three types of violations: Minor Violations, Major Violations, and Severe Violations.

1. **Minor Violations**
   Minor violations include but are not limited to:
   - Ceasing Data Entry
   - Failure to resolve Data Quality Errors
   - Failure to enter data in a timely manner
   - End User Inactivity
   - Failure to use an up-to-date browser
   - End User or Security Officer absent from a required annual Security and Privacy Awareness Training, unless prior arrangements have been made for receiving missed training
   - Minor failure to comply with requirements listed in Physical and Technical Safeguards

Sanctions for minor violations are dependent on the number of minor violations by the Participating Agency within a 12-month period.

First violation
A letter documenting violating event and involved personnel will be sent to the Participating Agency from the HMIS Lead and kept on file with the HMIS Lead. The Participating Agency must submit to HMIS Lead a written plan for corrective action, including any internal actions taken against the employee who violated policy, within 10 business days and complete the corrective action within 30 days.

Second violation
A letter as described in "First violation" above.

HMIS Lead will conduct a mandatory training session on security and privacy policies for the Participating Agency in question. This training must be attended by all End Users, the Agency's Security Officer, and the Agency Security Officer's Supervisor or Agency CEO/Executive Director. In organizations where the Agency Security Officer is the CEO/Executive Director, the training must be attended by the chair or president of the Agency's board of directors.

2. **Major Violations**
   Major violations include but are not limited to:
   - Failure to attend the annual Security and Privacy Awareness Training
   - Failure to respond to HMIS Lead Requests
   - *Sharing of Client PPI Via unsecure means of communication such as unencrypted email, etc.
   - Other violations of Policies

- *Failure to communicate in a timely manner when a staff is no longer employed, and access needs removed from the system
- Connecting to unsecure WI-FI
- Failure to use a firewall or virus protection
- Accessing the HMIS in a public location
- Failure to post the required notice of collection in intake/high-traffic areas
- *Failure to secure Client files
- Saving/storing password in internet browser
- Failure to set devices accessing the HMIS to automatically lock due to inactivity
- *Failure to report security and privacy incidents
- Failure to participate in a Security Review requested by HMIS Lead
- Major failure to comply with requirements listed in Physical and Technical Safeguards
- Accumulated minor violation issues:
    - Three or more minor violations within a 12-month period
    - Failure to submit a written plan for corrective action for minor violations within 10 days
    - Failure to complete corrective action for minor violations within 30 days

Sanctions for a major violation are:

- A letter as described in "First violation" for minor violations above;
- A mandatory training for all End Users and the Agency Security Officer
- An onsite security audit will be conducted by the HMIS Lead within 30 days of violation

3. **Severe Violations**

Severe violations include but are not limited to:

- Allowing non-authorized users to view any data from, have access to, see the screens of, or be provided any printouts of client data from HMIS
- *Sharing of Client PPI Via unsecure means of communication such as unencrypted email, etc.
- Other serious infractions that result in a compromise of the Member Agency and/or any client level data in the system
- Knowingly inputting inaccurate or false data into the HMIS System
- *Failure to complete corrective action plan
- *Failure to report security or privacy incidents
- Leaving account credentials in plain view or unattended
- Improper access of client data beyond scope of work or role
- *Failure to communicate in a timely manner when a staff is no longer employed, and access needs removed from the system

- *Failure to secure Client files
- Three or more major violations within a 12 month time period
- Sharing End User accounts
- End Users leaving HMIS account credentials in plain view or unattended
- Improper access of client data beyond the scope outlined in NMIS Policies and Procedures and this Plan

Sanctions for a severe violation are:

- A letter as described in "First violation" for minor violations above
- A mandatory training as described in "Second violation" for minor violations above
- The End User violating the policy or procedure will be prohibited from accessing HMIS or participating in HMIS data collection for 60 days. The Participating Agency remains responsible for meeting data quality and other obligations during this 60-day period.

HMIS Technical Support Protocol

The System Administrators will provide a reasonable level of support to Participating Agencies via email, phone, and/or remote.

1. End Users should first seek technical assistance/support from their Agency Administrator.
2. If more expertise is required to further troubleshoot the issue, the Agency Administrator or End User should submit a request to:

CCFL:

Balance of State CoC	Lincoln CoC
Bre Crow	Ciara Orr
bcrow3@unl.edu	corr14@unl.edu
402-472-3479	402-472-8332

CAN (only for CAAs):
Larissa Thomas
systemadmin@canhelp.org
402-471-3714 Ext. 2

3. Provide issue replication details if possible (or help recreate the problem by providing all information, screenshots, reports, etc.) so System Administrators can recreate the problem if required.
4. The System Administrators will try to respond to all email inquiries and issues within two business days, but support load, holidays, and other events may affect response time.
5. The System Administrator will submit a ticket to the software vendor as appropriate.

DATA QUALITY PLAN

This plan is designed to establish Data Quality standards for participating agencies within the Nebraska Balance of State and Lincoln CoCs HMIS System.

HMIS Data Quality Standards §580.37. The data quality standards ensure the completeness, accuracy, and consistency of the data in HMIS. The Continuum of Care is responsible for the quality of the data produced.

There are four necessary components to maintaining data quality: timeliness, completeness, accuracy, and consistency of data entry.

Timeliness

Entering data in a timely manner reduces human error that occurs when too much time has lapsed between the collection and/or service transaction and the data entry. Timely data also ensures community data accessibility.(e.g. monitoring purposes, increasing awareness, meeting funding requirements etc.)

Expectation: Each program type enters applicable data as soon as possible but must not exceed the prescribed timeframe.

Data Entry Timeframe		
Program Type	Minimum Data Elements	Timeframe Entry
Emergency Shelters:	Universal Data Elements; Universal Project Stay Elements; E*nrollments*; Services; *Assessments, if applicable; Exits*	Same day
Transitional Housing Programs	Universal Data Elements; Universal Project Stay Elements; E*nrollments*; Services; *Assessments, if applicable; Exits*	0-3 calendar days; Same day strongly preferred
Permanent Supportive Housing Programs	Universal Data Elements; Universal Project Stay elements; Enr*ollments;* Exits; Household Move-in Date; Services; Annual and Status updates	0-3 calendar days; Same day strongly preferred
Rapid Re-Housing Programs	Universal Data Elements; Universal Project Stay Elements; Enrollments; Exits; Household Move-in date; Services; Annual and Status Updates	0-3 calendar days after enrollment/eligibility is established; Same day strongly preferred
Homelessness Prevention Programs	Universal Data Elements; Universal Project Stay Elements; Enrollments;	0-3 calendar days after enrollment/eligibility is established; Same day strongly preferred

	Exits; Assessments; Services	
Street Outreach Programs	Enrollments; Exits; Services; Assessments	2 working days; Same day strongly preferred
Service Only	Universal Data Elements; Enrollments; Exits; Services; Assessments	7 calendar days; Same day strongly preferred

(Table A)

Completeness

All data entered into HMIS must be complete. Partially complete or missing data can negatively affect the ability to provide comprehensive care to clients. Missing data could mean the client does not receive needed services.

The Continuum of Care's goal is to collect 100% of all data elements. However, the CoC recognizes that this may not be possible in all cases, therefore, an acceptable range of null/missing and don't know/refused responses has been established based on the data element and type of program entering data.

Acceptable Range(s) of Data Completeness						
	TH, PSH, HUD SSO, RRH, HP		ES, Non-HUD SSO		Outreach	
Data Element	Missing	Unknown	Missing	Unknown	Missing	Unknown
First & Last Name	0%	0%	0%	0%	0%	0%
SSN	0%	5%	0%	5%	0%	5%
Date of Birth	0%	5%	0%	5%	0%	5%
Race and Ethnicity	5%	5%	5%	5%		
Sex	5%	5%	5%	5%		
Veteran Status	5%	5%	5%	5%		
Disabling Condition (Adults)	5%	5%	5%	5%		
Residence Prior to Entry	5%	5%	5%	5%		
Zip of Last Perm. Address	5%	5%	5%	5%		
Housing Status (Entry)	0%	5%	0%	5%		
Income & Benefits (Entry)	0%	5%	0%	5%		
Income & Benefits (Exit)	0%	5%	0%	5%		
Additional UPSEs (Adults; Entry)	0%	5%	0%	5%		
Destination (Exit)	0%	5%	0%	5%		

(Table B)

Bed Count and Utilization: Agency Administrators will report any changes to bed and unit counts to the HMIS Lead within 4 days of the change. Participating Agencies will promptly exit clients from beds and units in HMIS when clients leave projects. Maintaining accurate records of bed and unit counts in HMIS as well as accurate records of client bed and unit usage allows HMIS to accurately report utilization. Projects are expected to meet CoC-established utilization targets.

Accuracy

Participating Agencies are responsible for the accuracy of the data they enter into the HMIS. Accurate data provides a view of homelessness and the services provided by a community

Imprecise or false data creates an inaccurate picture of homelessness within a community and may create or diminish gaps in services. Inaccurate data may be intentional or unintentional. In general, false or inaccurate information is worse than incomplete information, since with the latter, it is at least possible to acknowledge the gap.

It should be emphasized to clients and staff that it is better to enter nothing than to enter inaccurate information. All data entered into the HMIS is a reflection of information provided by the client, as documented by the intake worker or otherwise updated by the client and documented for reference.

Expectation: Agency Administrators will check accuracy and consistency of data by running monthly program reports to ensure that the data "flows" in a consistent and accurate manner. For example, the following instances will be flagged and reported as errors:

- Mismatch between exit/entry data
- Co-enrollment or overlapping enrollment in the same program type
- Conflicting assessments
- Household composition errors

Participating Agencies agree to:

- Assure the accuracy of information entered into the system. Any updates in information, errors or inaccuracies that come to the attention of the participating agency will be corrected by said agency.
- Run the HUDX-225 HMIS Data Quality Report, HUDX-227 Annual Performance Report for CoC-funded programs, and HUDX-228 ESG CAPER for ESG- and NHAP-funded programs to monitor data and promptly correct inaccuracies by the 5th working day of each month for the previous month.

Agency Administrator:

- Runs and reviews reports in HMIS such as the APR, Universal Data Quality, Program Roster, etc., to include all participating programs
- Compares any missing rates to the data completeness benchmarks
- Emails the summary report and any related client detail reports to the System Administrator during the first week of the following Quarter?
- Improves their data completeness rate or provides explanation before the next - quarter's report.

Agency Administrator Report Expectations		
Report	If annual number of clients served <=50	If annual number of clients served >50
HUDX-225-HMIS Data Quality Report	Monthly	Weekly
HUDX-227-Annual Performance Report (for CoC-funded Programs)	Monthly	Weekly
HUDX-228-ESG CAPER Report (for ESG- and NHAP-funded Program)	Monthly	Weekly
GNRL-106 Program Roster Report	Monthly	Weekly
DQXX-102 Program Data Review	Monthly	Monthly
Pull 10% of paper files and check against HMIS data to verify accuracy	Monthly	Weekly
Issue a DQ report to program directors DQXX-103 Monthly Staff Report?	Monthly	Weekly

System Administrator:

- Run monthly data quality reports and send to agencies to fix data issues by the 5th of each month for the prior month.
    - Housing Project overlapping enrollments
    - Active clients missing ROIs
    - Missing move-in dates for PSH and RRH projects
    - Housing Project exits to "Other" Destination
- Run data quality monitoring reports as needed-contacts Agency Administrator or End User regarding data entry quality
- Reviews reports and assists the agency regarding any issues
- Reports persistent issues to Participating Agency Executive Director for advisement

Compliance

Data Timeliness: The average timeliness rate in any given month should be within the allowed timeframe. (See Table A)

Data Completeness: There should be no missing (null) data for required elements. Responses that fall under unknown (don't know or refused) should not exceed the allowed percentages. (See Table B and C)

Data Accuracy: The percentage of client files with inaccurate HMIS data shall not exceed 10%. For example, if the sampling includes 10 client files, then 9 out of 10 of these files must have the entire set of corresponding data entered correctly in HMIS.

Consistency

Consistency reflects that the use of HMIS is a standard operating procedure at Participating Agencies. Consistency in data collection and entry into the HMIS supports completeness and uniformity of the data collected, timeliness and efficiency of data entry, and accuracy of data recorded in the HMIS. Consistency is especially important where, as in Coordinated Entry, multiple Participating Agencies collect and enter the same data for the same purposes. Consistency is strongest when End Users perform HMIS tasks frequently using the same processes.

Participating Agencies should provide support for their End Users by maintaining consistent processes and providing refresher training as necessary to adhere to those processes.

System Administrators may determine that a particular End User needs to be retrained and identify the training to be required. End Users who are not regularly accessing the HMIS will be considered for retraining. Any End User who does not access the system for at least 30 days should complete Privacy and Security training and ROI Consent and Informed Consent training as described in NMIS policies 206 and 405 unless excused from these trainings by a System Administrator. Any End User who does not access the system for at least 90 days will be set as inactive and must complete new user training before accessing the HMIS again.

Unduplication Requirements §580.33(c). An HMIS must be capable of unduplicating client records as established by HUD in notice.

Policy: to reduce the duplication of client records, Participating Agency End Users should (1) always search for the client in HMIS before creating a new client record (2) avoid adding client records as Anonymous.

Description: The burden of *not* creating duplicate records falls on each participating agency. The HMIS system does not prevent duplicate client records from entering the database, therefore it is up to each user to ensure every client is first searched for, and if not found, then added. Having multiple (duplicate) records on the database for a single client causes confusion and inaccurate information being stored.

Procedures:

1. When an End User is entering client data, the End User will first attempt to locate that client on the system by searching for them by either name (first, last, and middle), or social security number (SSN).
2. It may be possible that this person already exists, but if no matches are found on the database for this client, the End User can add the client and their basic Universal Data elements.

Best Practices:

1. Perform more than one type of search when attempting to find an existing record. Clients often do not use the exact same name that was previously

entered.
2. Using a field other than name, such as social security number, tends to be more accurate and not open for much interpretation.

Data collection requirements

Policy: Participating Agencies are required to attempt data collection on individuals who are homeless and/or who are receiving services from the agency.

Procedures:

1. For HMIS Purposes, HUD's minimum standards require that the following be completed for all CoC projects. Typically, this is done at intake and then may need to be done again at an interim timeframe and again at exit (See Appendix C). For non-CoC programs, the same Universal Data Elements (UDEs) will be gathered.

Required Data Elements

Universal Data Elements (One and Only One per Client Record)	**Universal Project Stay Elements (One or More Value(s) Per Client, One Value Per Project Stay)**
3.01 Name	3.08 Disabling Condition
3.02 Social Security Number	3.10 Project Start Date
3.03 Date of Birth	3.11 Project Exit Date
3.04 Race and Ethnicity	3.12 Destination
4.21 Sex	3.15 Relationship to Head of Household
3.07 Veteran Status	3.16 Enrollment CoC
Client location	3.20 Housing Move-In Date
	3.917 Prior Living Situation

General Data Collection Guidance
Universal Data Elements are required to be collected by all projects participating in an HMIS, regardless of funding source. Universal Project Stay Elements are required to be collected by projects receiving HUD, ESG, CoC, or NHAP funding. UDEs are required to have one response per *client*, regardless of how many project enrollments that client has in the system. If at any point the data in these elements are observed to be incorrect or outdated, the data must be corrected in the client record. The UPSEs are to be collected at least once per *project enrollment*. The timing of when the data are to be collected and about whom is noted in each data element.

Uses and Disclosures of Client Data
Collecting UDEs can lead to questions about entering client information into HMIS and client rights to privacy. Staff must make data collection easy to understand by providing clients with a written copy of the CoC's Privacy Notice on request, describing the notice in plain language, and posting a public statement about data collection and uses. Assuring and maintaining privacy and confidentiality helps build trust in using HMIS. The client always has a right to privacy and can refuse to provide their information without being denied service.

Client consent is not needed to enter client information into the HMIS. Projects are required by their funder to ask the client for specific information and to enter it into HMIS. Please note, however, that collecting the data and using or disclosing the data are different things, and that uses and disclosures not listed in the CoC's privacy notice require the client's consent.

Common Program Specific Data Elements Standards

The following Program Specific Data Elements are required by more than one Federal Partner:

4.02 Income and Sources	***4.09 Mental Health Disorder***
4.03 Non-Cash Benefits	***4.10 Substance Use Disorder***
4.04 Health Insurance	***4.11 Domestic Violence***
4.05 Physical Disability	***4.12 Current Living Situation***
4.06 Developmental Disability	***4.13 Date of Engagement***
4.07 Chronic Health Condition	***4.14 Bed-Night Date***
4.08 HIV/AIDS	***4.21 Coordinated Entry Activity***

Additional Resources

- HMIS Data Standards
- HEARTH-CoC Program Interim Rule; codified at 24 CFR Part 578
- Federal Register Proposed Rules December 2011
- Federal Register Final Rule December 4, 2015, 24 CFR Parts 91 and 578

Appendix A: Email Confidentiality Notice

Email Confidentiality Notice

IMPORTANT MESSAGE FOLLOWS: This message and its attachments are intended only for the individual to whom it is addressed. They are confidential and may contain legally privileged information. If you are neither the intended recipient nor the agent responsible for delivering the message to the intended recipient you are hereby notified that any dissemination of this communication is strictly prohibited and may be unlawful. If you feel you have received this communication in error please notify us immediately by return e-mail to the sender and delete it from your system. We thank you in advance for your cooperation.

Appendix B: Security and Privacy Checklist

Security and Privacy Checklist		
Privacy Notice Policy		
	1. Does your agency have the HMIS Notice of Privacy Practices posted at every place where intake occurs? • Provide pictures of these posted notices	❑Yes ❑No
	2. Is a copy of the Privacy Notice available upon client request?	❑Yes ❑No
	3. How many intake locations are within the agency?	
	4. Is the Privacy Notice/Policy posted on your website?	❑Yes ❑No
	5. What is the version date of the Privacy Notice/Policy?	
	6. Have all users completed Privacy Training and have documentation of training?	❑Yes ❑No
	7. Have you encountered a need for the Privacy Notice/Policy to be provided in other languages or formats? (Braille, audio or large print).	❑Yes ❑No Describe: _____
User Authentication		
	1. How many users are in your agency?	
	2. Do your users share usernames and passwords?	❑Yes ❑No
	3. Do your users keep usernames and passwords in locations accessible to others?	❑Yes ❑No
	4. Do your users use their internet browsers to store passwords?	❑Yes ❑No
Hard Copy and Data and Disposal		
	1. Does your agency have procedures in place to protect hard copy Protected Personal Information (PPI) generated from or for the HMIS?	❑Yes ❑No
	2. Are all users trained on how to protect and dispose of hard copy data? If so, what is the procedure?	❑Yes ❑No
	3. Do you keep hard copy files in a locked drawer(s) or file cabinet(s)?	❑Yes ❑No
	4. Are the hard copy files kept in locked offices?	❑Yes ❑No
	5. What is your disposal policy? (Shredding of paper hard copy, reformatting of disks, etc.). • Provide a copy of your data and document disposal or retention policy	❑Yes ❑No
	6. How is client data generated from HMIS? (Printed screenshots, HMIS client reports, downloaded data into Excel, etc.).	
Physical Access		
	1. Are all devices accessing the HMIS in secure locations or are they attended at all times if they are in publicly accessible locations? (This includes other devices if they are networked with devices accessing the HMIS).	❑Yes ❑No
	2. Are devices accessing the HMIS positioned so that their screens are not easily visible?	❑Yes ❑No
	3. Do devices accessing the HMIS in open areas employ visual filters to prevent unauthorized viewing of information on the screen?	❑Yes ❑No

	4. Are your devices set to automatically lock due to inactivity?	❑Yes ❑No
	5. Are printers that are used to print hard copies from HMIS in secure locations?	❑Yes ❑No
	6. Are End Users permitted to access HMIS from outside the workplace? If so, does your agency have a remote data access policy? • Provide a copy of your remote data access policy	❑Yes ❑No ❑Yes ❑No

If your agency has an IT person, please forward questions concerning Virus Protection, Firewall, and Software Security to him or her. On the day of the Audit, CCFL will need to speak with your IT person regarding these questions or be provided with written responses from and including any printed verification that virus protection and firewalls are up to date.

IT Security		
Randomly select the larger of 10% or 3 of the devices used to access the HMIS. Use these devices to create documentation of virus protection, firewall, and software security compliance. If you have written IT policies and procedures governing virus protection, firewall, software security, and installing updates, provide a copy.		
Virus Protection		
	1. Are your devices networked?	❑Yes ❑No
	2. Do all of your devices have virus protection with automatic updates? (This includes other devices if they are networked with devices accessing HMIS). • Submit proof of the virus protection installed, including version number, whether the virus protection product is set to automatically update its definitions, and the most recent date the virus protection product was updated.	❑Yes ❑No
Firewall		
	1. Do you have a firewall on the network and/or devices(s) to protect HMIS systems from outside intrusions? • Report the model and version number of the firewall. • Submit screen shots verifying that the firewall is turned ON. • Document the most recent date the firewall was updated.	❑Yes ❑No
Software Security		
	1. Do all your devices accessing HMIS have current operating systems and current internet browsers? (This includes other devices if networked with devices accessing HMIS). • Document that all operating systems are up-to-date and the most recent date they were updated. • Document that all computers have a modern browser installed (such as Firefox, Chrome, Edge,	❑Yes ❑No

	Safari), that the browser is up-to-date, and the most recent date it was updated.	
Client Consent		
	1. Do all households entered into the HMIS have signed client consent on file? • Randomly select 10 client files and document that consent on file is accurately entered into Clarity.	❑Yes ❑No
	2. Where are the NMIS client consent forms kept? (Household paper file, common storage box/drawer, etc.).	❑Yes ❑No
HMIS Agreements		
	1. Has your agency signed and submitted the Agency Partner Agreement? • If your agency hasn't signed the Agency Partner Agreement, we will have copies to distribute on the day of the audit/assessment.	❑Yes ❑No
	2. Does your agency have copies of signed sharing agreements for all agencies you share data with? • Provide a list of agencies you share data with. • Provide a copy of your signed sharing agreements.	❑Yes ❑No
	3. Do you collect Releases of Information for clients to give consent to the sharing of their information with your partners in the agency sharing agreements? • Provide samples of your ROIs for your sharing agreements.	❑Yes ❑No
Date of Audit Completion:		
Signature of Security Officer:		
Agency Name:		
Name and Signature of Executive Director:		

Appendix C: Collection Points for HUD Data Elements

This content may be modified and reposted once it is in compliance, and the information will be updated again in the document.

Acknowledgment of Receipt of HMIS Security, Privacy, and Data Quality Plan

The HMIS Security, Privacy and Data Quality Plan contains important information regarding the expectations of agencies that use the Nebraska Management Information System.

_____I acknowledge that I have received a copy of the HMIS Security, Privacy and Data Quality Plan. I understand that it is my responsibility to read and comply with 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 immediate supervisor.

_____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 to adhere to the changes in the Plan as they occur.

Signature:_____ Date:_____

Document History

Date of Revision	Document Version #	Revision Notes
July 2016	1.0	First Release of Document
May 2023	1.1	Updated per HUD Data Standard release
September 2024	2.0	Major revision; updates to match NMIS SOP and new software.
May 2025	2.1	Replacement of 3.06 Gender with 4.21 Sex
March 2026	2.2	Annual Review