HMIS Security, Privacy and Data Quality Plan

This plan works in conjunction with the Nebraska Management Information System Policies and Standard Operating Procedures Manual and the HUD HMIS Data Standards and Federal Register Vol. 76 Subpart D-HMIS Governance, Technical, Security, and Data Quality Standards.

Operation of HMIS involves partnerships between MACCH CoC, HMIS Lead Agency, and Contributing HMIS Organizations (CHOs).

HMIS Security, Privacy and Data Quality Plan

Metro Area Continuum of Care (MACCH)

The Nebraska Management Information System (NMIS) is a locally administered electronic data collection system that stores longitudinal person-level information about the men, women, and children 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 serves as the foundation on which MACCH can plan and prepare to prevent, reduce and eliminate homelessness.

Because MACCH receives HUD Continuum of Care (CoC) funding, it 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 directly related 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. In August 2017, HUD Published changes in the HMIS Data Standards Revised Notice incorporating additional data collection requirements, this plan will try to incorporate these expectations.

"Being homeless is not job specific. It doesn't spare gender, age, race or ethnicity. It is equal opportunity misery. " (quote from the Milwaukee Guest House)

The intent of this plan is to set forth policies and procedures for MACCH and all Contributing HMIS Organizations (CHOs) to be in compliance with the HUD Federal regulations regarding:

- HMIS Technical Standards (Federal Register Vol. 76, No. 237 §580.33)
- HMIS Security Standards (Federal Register Vol. 76, No. 237 §580.35)
- Data Quality Standards (Federal Register Vol. 76, No. 237 §580.37)
- 2017 HMIS Data Standards (Version 1.3 April 2017)

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

- The Final Revised HMIS Data Standards; April 2017
- The Department of Housing and Urban Development Homeless Management Information Systems (HMIS); Data and Technical Standards Final Notice; Notice

- Nebraska Management Information System Policies and Standard Operating Procedures Manual

Table of Contents

DEFINITION OF TERMS

Annual Homeless Assessment Report (AHAR) HUD's annual report to Congress on the nature and extent of homelessness nationwide.

Annual Performance Report (APR) A reporting tool that HUD uses to track program progress and accomplishments of HUD homeless assistance programs on an annual basis (Formerly known as the Annual Progress Report).

Client A living individual about whom a Contributing HMIS Organization (CHO) collects or maintains protected personal information (1) because the individual is receiving, has received, may receive, or has inquired about services from CHO or (2)in order to identify services, needs, or to plan or develop appropriate services within the CoC.

Contributing HMIS Organization (or CHO) Any organization (employees, volunteers, and contractors) that records, uses or processes Protected Personal Information. This is what we commonly refer to within HMIS as an Agency and includes all associated staff.

Continuum of Care (CoC) 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 Recipient A person who obtains PPI from an HMIS Lead Agency or from a CHO for research or other purpose not directly related to the operation of the HMIS, CoC, HMIS Lead Agency, or CHO.

Homeless Management Information System (HMIS) 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 Agency means an entity designated by the Continuum of Care in accordance with HUD to operate the Continuum's HMIS on its behalf.

HMIS Software Solution Provider An organization that sells, licenses, donates, builds or otherwise supplies the HMIS user interface, application functionality and database.

HMIS Participating Bed For any residential homeless program, a bed is considered a "participating HMIS bed" if the program makes a reasonable effort to record all universal data elements on all clients served in that bed and discloses that information through agreed upon means to the HMIS Lead Agency at least once annually.

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, 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 CHOs who assist in making decisions regarding the HMIS system, HMIS policies and procedures, and any concerns that arise regarding it.

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

Longitudinal System Analysis (LSA) is produced from the a CoC's Homeless Management Information System and submitted annually to HUD via the HDX 2.0, provides HUD and Continuums of Care with critical information about how people experiencing homelessness use their system of care.

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.

Protected identifying information(PPI) means any information about a client that (1) identifies a specific individual, (2) can be manipulated so that identification is possible, (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.

System Performance Measures (SPM) are system-level performance information reports used by HUD as a competitive element in its annual CoC Program Competition and to gauge the state of homeless response system nationally.

Unduplicated Accounting of Homelessness An unduplicated accounting of homelessness includes measuring the extent and nature of homelessness (including an unduplicated count of homeless persons), utilization of homelessness programs over time, and the effectiveness of homelessness programs.

Unduplicated Count of Homeless Persons An enumeration of homeless persons where each person is counted only once during a defined period of time.

Victim service provider means a private nonprofit organization whose primary mission is

to provide services to victims of domestic violence, dating violence, sexual assault, or stalking. This term includes rape crisis centers, battered women's shelters, domestic violence transitional housing programs, and other programs.

HMIS Technical Standards §580.33

"HMIS Leads and HMIS Vendors are jointly responsible for ensuring compliance with the technical standards applicable to HMIS."

§580.33 (c): An HMIS must be capable of un-duplicating client records as established by HUD.

Policy: in order to reduce the duplication of client records, CHO Users should (1) always search for the client in HMIS before creating a new client record (2) avoid using the 'Anonymous' button.

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 CHO user is collecting data from a client, the CHO 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 CHO 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 tends to be more accurate, and not open for much interpretation (social security number).

§580.33 (d): Data collection requirements. (1) Collection of all data elements. An HMIS must contain fields for collection of all data elements established by HUD.

Policy: Agencies/CHO's 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. For Non-CoC programs, the expectation is that the same Universal Data Elements will be gathered.

Required Data Elements

Universal Data Elements: Required for all individuals in all program types
Name
Social Security Number
Date of Birth
Race
Ethnicity
Gender
Veteran Status
Disabling Condition
Program Start Date
Program Exit Date
Destination
Relationship to Head of Household
Client Location
Housing Move-in Date
Living Situation

Program Specific Data Elements Standards (See HUD's 2017 Data Standards)

Income and Sources
Non-Cash Benefits
Health Insurance
Disabling Condition
Domestic Violence
Contact (Outreach only)
Date of Engagement (Outreach only)
Housing Assessment Disposition (Homeless prevention only)

As per the NMIS Policies and Procedures Manual all agencies that use HMIS must complete the Nebraska Universal.

HMIS Security Standards §580.35

"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 government requirements.

If a CHO is subject to federal, state, or local laws that require additional confidentiality protections, the CHO must comply with those laws. The HMIS standards do not exempt CHOs from other laws. In developing a privacy notice, each CHO should make appropriate adjustments required any other applicable laws.

All HMIS Leads, CHOs, and HMIS vendors must follow the security standards established by HUD, and the HMIS Lead must develop a security plan.

SECURITY AND PRIVACY PLAN

This plan is designed to establish security and privacy standards for participating agencies within the Nebraska MACCHBook/IICA HMIS System. The following requirements and recommendations are based on the Security Standards as defined in the Federal Register/Vol. 76, No. 237. The goal is to support and assist CHO's in meeting these requirements. 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 participating agencies will follow the following levels of security:

- Ensure the confidentiality, integrity, and availability of all HMIS information
- Protect against any reasonable anticipated threats to security
- Ensure compliance by End Users

HUD Minimum Requirements

1. **HMIS Security Officer**
   The HMIS Lead must designate one staff member as the HMIS Security Officer. Each CHO must also designate a HMIS Security Officer to be responsible for ensuring compliance applicable security standards within the CHO. The CHO Security Officer does not need to be an End User but they must be an employee of the CHO. For any CHO without employees, the HMIS Security Officer must be the President, Chair, or other top-level representative responsible for the CHO.

2. **Workforce Security**
   Each CHO must have a workforce security policy that includes conducting a criminal background check on its HMIS Security Officer and on any users with Agency Administrator level access or greater. Criminal Background checks must be

completed at least once. On request, CHOs must verify to HMIS when the most recent criminal background check has been completed for each applicable staff member. The background check must include local and state records; CHOs are strongly encouraged to include federal records as well, but are not required.

3. Security and Privacy Awareness Training and Follow-up

The HMIS Lead will conduct a 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.

4. Reporting Security Incidents

Any End User or Security Officer suspecting violations of Security and Privacy policies should report incidents in writing. (See Appendix for Incident Report)

Chain of Reporting: End Users should report issues first to their CHO's designated Security Officer within one business day. Security Officers should report the issue jointly to the CHO Director and the Lead HMIS Staff within one business day.

5. Disaster Recovery Plan

The Disaster Recovery Plan for HMIS is the responsibility of our HMIS Vendor, Bowman Systems, which hosts and houses the data on remote servers. The vender, Bowman Systems 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, HMIS Lead will contact CHO Security Officers by phone or email within one business day to inform them of the expected scale and duration of the loss or downtime.

6. Annual Security Review

All CHOs must undergo an annual security review, which will include at minimum the completion of a Security Checklist (See Appendix) Agency Administrators will work with the CHO Security Officer to schedule an audit and will assist with performing the review. The results of the annual review must be returned to the HMIS Security Officer via Fax or Email the same day they are completed. Any items needing to be fixed must be fixed within 10 working days.

7. Contracts and other arrangements

The Lead HMIS 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.

§580.35 E & F Physical & Technical Safeguards

The purpose of Physical safeguards is to ensure that access to data in HMIS is protected and meets baseline security standards. All HMIS Leads and CHOs must follow the standards below.

- All HMIS workstations must be placed in secure locations or must be manned at all times if they are in publicly accessible locations. (This includes non-HMIS computers if they are networked with HMIS computers).
- All printers used to print hard copies from the HMIS are in secure locations.
- All HMIS workstations must use password protected screensavers after five or more minutes of inactivity.
- All HMIS workstations must have a password protected log on for the workstation itself.
- All HMIS End User's computer screens should be placed in a manner where it is difficult for others to see the contents or must have a screen protector.
- Passwords must be memorized, not written down and should not be shared.
- Confidential data CANNOT be stored on ANY unencrypted mobile device.
- Confidential data CANNOT be transmitted via unencrypted wireless devices or unsecured public lines.
- Internet browser must be compatible with 128-bit encryption.
- Internet browser must be a current/most up-to-date version
- HMIS should not be access via unsecured wi-fi or other unsecured internet connection.
- Any e-mail containing confidential data must utilize at least 128-bit encryption.
- All email messages must contain a Confidentiality Notice. (See Appendix)
- All HMIS Workstations must have an active Firewall turned on.
- All HMIS equipment must have approved anti-virus software installed and configured to automatically download current signature file.
- Anti-virus software must be set to scan emails file downloads in real time.
- HMIS agencies must have their entire Network behind a firewall and must routinely monitor for intrusion attempts.
- All Windows based computing equipment must have Microsoft Updates set to automatically download and install any critical update.
- All HMIS workstations must be running a current operating system and internet browser security.
- Systems must be scanned at minimum of weekly for viruses and malware.
- End Users who have not logged onto the system in the previous 90 days will be flagged as inactive.
- Under no circumstances shall a CHO demand that an End User hand over his or her username and password.

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."

This plan is designed to establish Data Quality standards for participating agencies within the Nebraska HMIS System.

Participating Agencies/CHOs 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 Data Quality Report 252 Data Completeness Report Card (EE) for programs that do an entry/exit and run the 243 Data Completeness Report Card (Svs) for Service Only programs from HMIS to monitor data and promptly correct inaccuracies by the 5th working day of each month for the previous month.

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

1. **Timeliness**

   ICA, on behalf of MACCH and its members, must create aggregate monthly, quarterly, and annual reports for our community and for the Federal Department of Housing and Urban Development (HUD). Reliable aggregate reports are only feasible when all relevant data is entered and verified BEFORE aggregate reports are created. That means all HMIS client encounter data must be entered into the HMIS in a timely manner to ensure that all clients served in that time period are included in each report. MACCH also stipulates that the minimum requirements below do NOT override any additional or more stringent data requirements of program funders or directors. The ultimate goal of the CoC is to move toward real-time use of HMIS data for checking bed availability, program eligibility, and referral/service confirmation.

   To achieve that goal, agencies are encouraged to enter intake, entry/exit, or service data as soon as possible. Real-time data entry is ideal. The CoC minimum data requirements do NOT override or replace any additional date required by various funders. The following minimum HMIS date entry timeliness benchmarks are established for:

Data Entry Timeframe		
Program Type	Minimum Data Elements	Timeframe Entry
Emergency Shelters:	Nebraska Universal, Housing Check-In/Check-Out, Services	4 calendar days
Transitional Housing Programs	Nebraska Universal, Program Entry/Exit, Services	4 calendar days
Permanent Supportive Housing Programs	Nebraska Universal, Program Entry/Exit,	4 calendar days

	Services	
Rapid Re-Housing Programs	Nebraska Universal, Program Entry/Exit, Services	4 calendar days after enrollment/eligibility is established
Homelessness Prevention Programs	Nebraska Universal, Program Entry/Exit, Services	4 calendar days after enrollment/eligibility is established
Outreach Programs	Nebraska Universal, Services	4 working days

(Table A)

2. **Completeness**

This benchmark requires that, for all clients giving informed consent, data on 100% of those provided homeless services will be entered into the HMIS. In addition, it is also expected that all Nebraska Universal* and Project-Specific Data Elements are completed as required and defined by HUD. Where there are situations in which responses to certain data elements cannot be determined, exceptions to these expectations will be acceptable. However, these exceptions are defined in the benchmark as limited to an acceptable range of null/missing and unknown/don't know/refused responses. Data for all consenting persons receiving homeless support from HMIS participating programs will be collected and entered into the HMIS system. This includes all Nebraska Universal Data Elements* and any Project-Specific Data Elements required by HUD for each type of project.

Exceptions:

- Agencies/Projects working with Domestic Violence clients will record the equivalent data in an internal data collection system.
- Data elements recorded as null/missing will not exceed five percent (5%) of the total number of records for program participants in the period being reported.
- Data elements recorded as unknown/don't know/refused will not exceed ten percent (10%) of the total number of records for participants in the period being reported.

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	5%	5%	5%	5%	5%	5%
Date of Birth	5%	5%	5%	5%	5%	5%
Race	5%	5%	5%	5%	5%	5%
Ethnicity	5%	5%	5%	5%	5%	5%
Gender	5%	5%	5%	5%	5%	5%
Veteran Status (Adults)	5%	5%	5%	5%	5%	5%
Disabling Condition	5%	5%	5%	5%	5%	5%
Destination	5%	5%	5%	5%	5%	5%

Relationship to HoH	5%	5%	5%	5%	5%	5%
Housing Move-in Date	5%	5%	5%	5%	5%	5%
Living Situation	5%	5%	5%	5%	5%	5%
Add'l PDEs (Adults; Entry)	5%	5%	5%	5%	5%	5%
Destination (Exit)	0%	5%	0%	5%	**5%**	5%

(Table B)

Bed Count: Agency Administrators should periodically update bed and unit counts in the HMIS database to ensure accuracy.

Data Entry Timeframe for Bed Counts	
PROGRAM TYPE	TIMEFRAME ENTRY
Emergency shelters	monthly, within 4 days of the month's end
Scattered-site programs (TH or PH)	quarterly, within 4 days of the month's end
Project-based program	annually, within 4 days of the contract end date

Bed Utilization Rate: Upon exiting a program, the End-User exits the client from the bed or unit in the HMIS. The acceptable range of bed/unit utilization rates for established projects is:

Bed Utilization Rate (Calculated Beds available/Beds used)	
PROGRAM TYPE	PERCENTAGE UTILIZED
Emergency shelters	65% - 105%
Transitional Housing/Permanent Support Housing	65% - 105%
Rapid Rehousing	65% - 105%

(Table C)

Exception: New projects may require time to reach the projected occupancy numbers, the bed utilization rate requirement will be relaxed during the first operating year.

3. Accuracy

CHO's/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 within the BOS.

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 quarterly 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

§580.37 D 1 Data Quality Plan

The HMIS Lead Agency will work with System Administrators to set a schedule to annually monitor each participating agency to ensure data quality. Roles and responsibilities of monitoring are outlined in this section.

Agency Administrator:

- Runs and reviews reports in ART such as the APR, ESG CAPER, 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 by the 5th business of the following month
- Improves their data completeness rate or provides explanation before the next month's report.

System Administrator:

- 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 CHO Executive Director for advisement

Agency Administrator Report Expectations		
Report	If annual number of clients served <####	If annual number of clients served >###
Run 0216 – Unexited Client Exceeding Max Length of Stay Report Exit cases that should be closed Enter cases that should be open	Monthly	Weekly

Run 214 Universal Data Element Completeness (closed) Or 215 Universal Data Element Completeness (Open)	Monthly	Weekly
Run 0220 Data Incongruity Locator	Quarterly	Quarterly
Pull 10% of paper files and check against HMIS data to verify accuracy	Monthly	Weekly
If shelter, run Bed List Report Verify accuracy against paper shelter list	Weekly	Weekly
If shelter, run Bed List Report Check Bed List to verify that number of open beds on HMIS reports equals number of households on Bed List	Monthly	Weekly
Issue a DQ report to program directors	Monthly	Weekly

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.

Required Data Elements

Universal Data Elements: Required for all individuals in all program types

Name
Social Security Number
Date of Birth
Race
Ethnicity
Gender
Veteran Status
Disabling Condition
Program Start Date
Program Exit Date
Destination
Relationship to Head of Household
Client Location
Housing Move-in Date

Living Situation

Program Specific Data Elements Standards (See HUD's 2010 Data Standards)

Income and Sources
Non-Cash Benefits
Health Insurance
Disabling Condition
Domestic Violence
Contact (Outreach only)
Date of Engagement (Outreach only)
Housing Assessment Disposition (Homeless prevention only)

APPENDIX

Documents

- Violations
- Email Confidentiality Notice

Action Items

- Security Check list
- Acknowledgement of Receipt of HMIS Plan

Additional Resources

- March 2017 Data Standards
- https://www.hudexchange.info/resource/3824/hmis-data-dictionary/
- HEARTH-HMIS Guidelines
  https://onecpd.info/resources/documents/CoCProgramInterimRule.pdf
- Federal Register Proposed Rules December 2011
  https://www.onecpd.info/resources/documents/HEARTH_HMISRequirementsProposedRule.pdf

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:

- End User or Security Officer's absence at a required annual Security and Privacy Awareness Training, unless prior arrangements have been made for receiving missed training.
- Workstations non-compliant with 3 or less Workstation Security items described in §580.35 E & F Physical & Technical Safeguards

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

First violation
A letter documenting violating event and involved personnel will be sent to CHO from HMIS Lead and kept on-file with HMIS Lead. CHO must submit to HMIS Lead a written plan for corrective action, including any internal actions taken against 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 CHO in question. This training must be attended by all end users, the CHO's Security Officer, and the Security Officer Supervisor or CHO executive director. In organizations where the Security Officer is the executive director, the training must be attended by the chair or president of the CHO's board of directors.

2. **Major Violations**
   Major violations include but are not limited to:

- 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
- Failure to conduct a criminal background check
- Failure to participate in an Annual Security Review
- Workstations non-compliant with 3 or more Workstation Security items
- Failure to report security and privacy incidents
- Transmitting Client Identifiers in plain text via unsecured or unencrypted e-mail

Sanction for a major violation is:

- A letter as described in "First violation" for minor violations above;
- A mandatory training for all HMIS end users
- An onsite security audit will be conducted by HMIS Lead within 30 days of violation

3. Severe Violations

Severe violations include but are not limited to:

- Three or more major violations within a 12-month time period
- Sharing ServicePoint End User accounts
- End users leaving ServicePoint account credentials in plain view or unattended
- Improper access of client data beyond the scope outlined in NMIS Policies and Procedures and this Plan

Sanction for a severe violation is:

- 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 ServicePoint or participating in HMIS data collection for 60 days. The CHO remains responsible for meeting data quality and other obligations during this 60 day period.

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/or by telephone at INSERT PHONE NUMBER HERE) and delete it from your system. We thank you in advance for your cooperation.

INSERT AGENCY/PROGRAM NAME HERE

Security and Privacy Checklist		
Data Collection		
	1. Are you using a paper intake form and if so, are you using the Nebraska Universal? If not, please provide us with a copy. (If no, skip to question 2) • If yes, ICA will ask to see the intake form • Agencies should be using the Nebraska Universal • Other paper forms need to be reviewed by ICA to make sure they are collecting the appropriate data elements	NMIS Policies and Procedures
	2. Are you collecting the Universal Data Elements on all clients? (Name, Social Security Number, Date of Birth, Ethnicity and Race, Gender, Veteran Status, Disabling Condition, Destination, Relationship to Head of Household, Client Location, Housing Move-in Date, Living Situation).	NMIS Policies and Procedures
	3. Are you collecting Program Data Elements? (All CoC funded, ESG funded, RHY funded, VA funded, PATH funded).	NMIS Policies and Procedures
	4. Are you monitoring data quality?	
	5. Have users been trained on how to collect data?	
Privacy Notice Policy		
	1. Does your agency have the HMIS Notice of Privacy Practices posted at every place where intake occurs? • ICA will need to visually confirm that both pages are posted.	§580.31(g)
	2. Is a copy of the Privacy Notice available upon client request?	
	3. How many intake locations are within the agency?	
	4. Is the Privacy Notice/Policy posted on your website?	
	5. What is the version date of the Privacy Notice/Policy?	
	6. Have all users completed Privacy Training and have documentation of training?	
	7. Have you encountered a need for the Privacy Notice/Policy to be provided in other languages or formats? (Braille, audio or large print).	
User Authentication		
	1. How many users are in your agency? • ICA will be spot checking for any visible usernames and passwords in drawers, on PC's, under mouse pads and keyboards, etc.	NMIS Policies and Procedures
	2. Do your users share usernames and passwords?	
	3. Do your users keep usernames and passwords in public locations?	
	4. Do your users use their internet browsers to store passwords?	
	5. All users have signed User Agreements/Confidentiality documents on file.	
Hard Copy and Data and Disposal		
	1. Does your agency have procedures in place to protect hard copy Personal Protected Information (PPI) generated from or for the HMIS?	§580.35
	2. Are all users trained on how to protect and dispose of hard copy data? If so, what is the procedure?	

	3. Do you keep hard copy files in a locked drawer(s) or file cabinet(s)? If so, • ICA will be looking for locked drawers/file cabinets in secured areas.	
	4. Are the hard copy files kept in locked offices?	
	5. What is your disposal policy? (Shredding of paper hard copy, reformatting of disks, etc.). • ICA will ask to see a written copy of procedures for client data disposal.	
	6. How is client data generated from HMIS? (Printed screen shots, HMIS client reports, downloaded data into Excel, etc.).	
	Physical Access	
	1. Are all HMIS workstation(s) in secure locations or are they manned at all times if they are in publicly accessible locations? (This includes non-HMIS computers if they are networked with HMIS computers). • ICA will be checking to see that computer screens are turned away from an open door. • If computers are in open areas, we will be checking for special screens that prevent unauthorized viewing of client information.	§580.35
	2. Are you utilizing password protected screensavers? • ICA will be checking for password protected screensavers.	
	3. Are printers that are used to print hard copies from HMIS in secure locations?	
	4. Are users able to access HMIS from outside the workplace? If so, does your agency have a data access policy?	

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, ICA 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.

	Virus Protection	
	1. Are your computers networked?	§580.35
	2. Do all of your computers have virus protection with automatic updates? (This includes non-HMIS computers if they are networked with HMIS computers). • ICA will be checking 10% of the computers or a minimum of 3 computers. • ICA will be checking and notating the most recent version of the virus protection software. (Symantec, Norton, McAfee, etc.). • ICA will be checking whether or not the virus Auto-Update is on. • ICA will be checking for the last date virus software was updated.	

Firewall		
	1. Do you have a firewall on the network and/or workstation(s) to protect HMIS systems from outside intrusions? • ICA will be checking firewall software. • ICA will be asking for printed screen shots to verify that the firewall is turned ON. • ICA will be asking for printed screen shots to verify that the firewall is updated.	§580.35
Software Security		
	1. Do all your HMIS workstation(s) have current operating systems and internet browser security? (This includes non-HMIS computers if networked with HMIS computers). • ICA will be checking for the latest operating system. • ICA will be checking for the latest internet browser (Mozilla Firefox, Google Chrome, etc.).	§580.35
Client Consent		
	1. Do all households entered into the HMIS have signed client consent from on file? • ICA will be conducting a random check of 10 client consent forms.	NMIS Policies and Procedures
	2. Where are the HMIS client consent forms kept? (Household paper file, common storage box/drawer, etc.).	
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.	§580.35 (d) (7)
	2. Does your agency have copies of signed sharing agreements for all agencies you share data with? • ICA will request a copy of the list of agencies you share data with and will want to review your signed sharing agreements.	
HMIS Barriers		
	1. Does your agency have barriers or challenges to entering HMIS data?	FR: None
	2. If so, what are they? (Not having enough time to enter data; staff needs more HMIS training; want to keep existing database and import later into HMIS, etc.).	
	3. Are you concerned about the confidentiality or security of HMIS data?	
	4. Are you aware of Techsoup.org?	

Acknowledgement 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:_____