SECURITY, PRIVACY AND DATA QUALITY PLAN

V1.1

Part of the *COHMIS Manual*

The *COHMIS Manual* comprises the Policies and Procedures as well as other documentation used to operate the Colorado Homeless Management Information System (COHMIS). These materials were developed by the Colorado HMIS Statewide Collaborative, which represents the state's HUD-designated Continuums of Care (CoCs). The CoCs maintain the COHMIS to help reduce homelessness in Colorado.

COHMIS Security, Privacy and Data Quality Plan

Table of Contents

Appendices

1. Introduction

The Colorado Homeless Management Information System (COHMIS) is a locally administered electronic data collection system that stores longitudinal person-level information about clients who access homelessness services and other human services in a community.

By streamlining and consolidating recordkeeping requirements, COHMIS allows service providers and stakeholders to provide an accurate and effective presentation of homelessness on program, agency, continuum, and statewide levels. The reports generated using COHMIS data serve as the foundation on which the State of Colorado and the Continuums of Care (as the Colorado HMIS Statewide Collaborative); can plan and prepare to prevent, provide and evaluate care to help reduce and eliminate homelessness. These reports may also assist in providing and evaluating care at an individual client level.

Because the Colorado CoC's receive 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 competition are directly related to a CoC's progress in ending homelessness, which is supported by data from the HMIS.

In the 2004 Federal Register, HUD published the HMIS Data and Technical Standards. These define the requirements for data collection, privacy safeguards, and security controls for all local HMIS systems. In March 2010, HUD published a Revised HMIS Data Standards Notice, incorporating additional data collection requirements. In April 2018, HUD updated changes in the HMIS Data Standards. This Security, Privacy & Data Quality Plan will incorporate expectations and changes as they are released from HUD.

The intent of this plan is to set forth Policies and Procedures for the Colorado HMIS Statewide Collaborative and Partner Agencies to be in compliance with the HUD Federal regulations regarding:

- HMIS Technical Standards (Federal Register Vol. 76, No. 237 §580.33), available at: https://www.hudexchange.info/programs/hmis/hmis-data-and-technical-standards/
- HMIS Security Standards (Federal Register Vol. 76, No. 237 §580.35), available at: https://www.hudexchange.info/resources/documents/HEARTH_HMISRequirementsProposedRule.pdf
- Data Quality Standards (Federal Register Vol. 76, No. 237 §580.37), available at: https://www.hudexchange.info/resources/documents/HEARTH_HMISRequirementsProposedRule.pdf
- 2020 HMIS Data Standards Manual (October 2019), available at: https://www.hudexchange.info/resource/3824/hmis-data-dictionary/

All persons using COHMIS are expected to read, understand, and adhere to:

- The 2020 HMIS Data Standards Manual (October 2019)
- The Department of Housing and Urban Development Homeless Management Information Systems (HMIS); Data and Technical Standards Final Notice; Notice (July 2004)
- COHMIS Policies & Procedures Manual 2020 (January 2020)

2. Definition of Terms

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 Partner Agency (PA) collects or maintains Personally Identifiable Information (1) because the individual is receiving, has received, may receive, or has inquired about services from PA or (2)in order to identify services, needs, or to plan or develop appropriate services within the CoC.

Comparable Database (CD): An information system for victim service providers to enter data and report on HUD requirements separate from HMIS, as required by VAWA.

Continuum of Care (CoC): A 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 Partner Agency Liaison (DPAL): An active user of HMIS who is designated to communicate and lead the effectiveness of HMIS at an agency level. Among other things, DPAL's are responsible for authorizing End Users and access levels in HMIS, running reports, leading internal audits, and reporting breaches in privacy or security to the Lead Agency.

Data Recipient: A person who obtains PII from an HMIS Lead Agency or from a PA for research or other purposes not directly related to the operation of the HMIS, CoC, HMIS Lead Agency, or PA.

Homeless Management Information System (HMIS): 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: 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: 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: The Department of Housing and Urban Development.

Agency Participation Agreement: A written agreement between the HMIS Lead Agency and each Partner Agency that details the responsibilities of each party regarding participation in HMIS.

Longitudinal System Analysis (LSA): A report that provides HUD and Continuums of Care (CoCs) with critical information about how people experiencing homelessness use their system of care. (Formerly known as the Annual Homeless Assessment Report (AHAR).

Partner Agency (PA): Any agency or organization (employees, volunteers, and contractors) that records, uses or processes Personally Identifiable Information (PII). This is what we commonly refer to within HMIS as an Agency and includes all associated staff.

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

Privacy Standards: Apply to all Agencies and Programs that record, use or process Personally Identifiable Information (PII) within the HMIS, regardless of funding source.

Personally Identifiable Information (PII): 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.

SAGE HMIS Reporting Repository: HUD has moved from E-snaps to SAGE, for APR reporting. Recipients are required to upload time-stamped Comma Separated Value (CSV) data from their HMIS/Comparable Database to fulfill the APR reporting requirement in SAGE. Recipients will not be able to manually enter data about participants served.

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

Unduplicated Count of Persons Experiencing Homelessness: An enumeration of persons experiencing homelessness, where each person is counted only once during a defined period of time.

Violence Against Women Act (VAWA): Law passed in 1994 and re-authorized thereafter, promoting a coordinated community response to domestic violence, sex dating violence, sexual assault, and stalking. VAWA also supports the work of community-based organizations that are engaged in work to end domestic violence, dating violence, sexual assault, and stalking; particularly those groups that provide culturally and linguistically specific services. VAWA has specific regulations prohibiting the entry of data into HMIS by victim service providers.

Victim Service Provider: 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.

3. HMIS Technical Standards §580.33

The CoC's are responsible for ensuring compliance with the technical standards applicable to HMIS.

3.1 *§580.33 (c):* An HMIS must be capable of un-duplicating client records as established by HUD

3.1.1 Policy
In order to reduce the duplication of client records, PA Users must always search for the client in HMIS before creating a new client record.

3.1.2 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.

3.1.3 Procedures
1. When a PA user is collecting data from a client, the PA user will first attempt to locate that client on the system by searching for them by either name (first, last, and middle), date of birth (DOB) 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 PA user can add the client and their basic Universal Data elements.

3.1.4 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 (i.e. social security number, date of birth, etc.).

3.2 §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.

3.2.1 Policy
Agencies/PA's are required to attempt data collection on individuals/households who are experiencing homelessness and/or who are receiving services from the agency.

3.2.2 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.
2. For Non-CoC programs, the expectation is that the same Universal Data Elements will be gathered for consistency and identifying duplicates across the system.

3.2.3 Universal Data Elements
Universal Identifier Elements:

3.01 Name
3.02 Social Security Number
3.03 Date of Birth
3.04 Race
3.05 Ethnicity
3.06 Gender
3.07 Veteran Status

Universal Project Data Elements:

- 3.08 Disabling Condition
- 3.10 Project Start Date
- 3.11 Project Exit Date
- 3.12 Destination
- 3.15 Relationship to Head of Household
- 3.16 Client Location
- 3.20 Housing Move-in Date
- 3.917 Prior Living Situation

3.2.4 Program Specific Data Elements

Common Program Specific Data Elements:

- 4.02 Income and Sources
- 4.03 Non-cash benefits
- 4.04 Health Insurance
- 4.05 - 4.10 Disability Elements
  - 4.05 Physical Disability
  - 4.06 Developmental Disability
  - 4.07 Chronic Health Condition
  - 4.08 HIV/AIDS
  - 4.09 Mental Health Problem
  - 4.10 Substance Abuse
- 4.11 Domestic Violence
- 4.12 Current Living Situation
- 4.13 Date of Engagement (Outreach only)
- 4.14 Bed-Night Date
- 4.19 Coordinated Entry Assessment
- 4.20 Coordinated Entry Event

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

All HMIS Leads, PAs, and HMIS vendors must follow the security standards established by HUD, and the HMIS Lead must develop a security plan. This security plan will be approved and overseen by the CoC.

4.1 Security and Privacy Plan

This plan is designed to establish security and privacy standards for participating agencies within the COHMIS 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 PA'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 reasonably anticipated threats to security
- Ensure compliance by End Users

4.1.1 HUD Minimum Requirements

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

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 DPALs. 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 COHMIS will be restricted until they participate.

Reporting Security Incidents: Any End User or DPAL suspecting violations of Security and Privacy policies should report incidents in writing. (See Appendices for Incident Report)

Chain of Reporting: End Users should report issues first to their DPALs within one business day. DPALs should report the issue jointly to the Partner Agency Director and the Lead HMIS Staff within one business day.

4.2 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 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 DPALs by phone or email within one business day to inform them of the

expected scale and duration of the loss or downtime.

4.3 Annual Security Review

All Partner Agencies must undergo an annual HMIS monitoring review, which will include at minimum the completion of a Security Checklist (See Appendix) DPALs will schedule an audit and will assist with performing the review. The results of the annual review must be returned to the DPAL and HMIS Lead Agency via Fax or Email the same day they are completed. Any items needing to be fixed must be fixed within 10 working days.
More information on the COHMIS Lead Agencies can be found via the link below:
https://cohmis.zendesk.com/hc/en-us/sections/360002795731-CoC-Information

4.4 Contracts and Other Arrangements

The Lead HMIS Agency 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.

5. Physical and Technical Safeguards §580.35

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

- All HMIS workstations must be placed in secure locations or must be occupied 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 lock screens after five minutes of inactivity.
- All HMIS workstations must have a password protected log on for the workstation itself.
- All HMIS end user computer screens must be placed in a manner where it is difficult for others to see the contents or must have a blackout filter.
- Passwords must be memorized, not written down in a publicly accessible location, and must never 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 must not be accessed via unsecured wi-fi or other unsecured internet connection
- Any email containing confidential data must utilize at least 128-bit encryption.
- 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.
- Antivirus software must be set to scan emails and 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 for viruses and malware weekly, at a minimum.
- End Users who have not logged onto the system in the previous 90 days will be flagged as inactive.
- Under no circumstances shall a Partner Agency demand that an end user hand over their username and password.

6. 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 ensuring HMIS data complies with these data quality standards.

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

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 Data Quality Report and Data Completeness Report Card from HMIS to monitor data and promptly correct inaccuracies by the 5th working day of each month for the previous month.
- Best Practice: Running reports more than once a month will assist agencies in avoiding the possibility of addressing numerous inaccuracies at month's end.

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

6.1 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 time frame.

Table A

Data Entry Time Frame

Program Type	Minimum Data Elements	Time Frame for Entry
Emergency Shelters	Housing Check-In/Check Out, Services	Same Day
Transitional Housing Programs	Program Entry/Exit, Services	7 Calendar Days
Permanent Supportive Housing Programs	Program Entry/Exit, Services	7 Calendar Days
Rapid Re-Housing Programs	Program Entry/Exit, Services	7 Calendar Days After Enrollment/Eligibility is Established
Homelessness Prevention Programs	Program Entry/Exit, Services	7 Calendar Days After Enrollment/Eligibility is Established
Outreach Programs	Services	2 Working Days

6.2 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. Additionally, incomplete data leads to inaccurate reporting at the program level and the system performance level.

The CoC'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.

Table B

Acceptable Range(s) of Data Completeness						
	TH, PSH, HUD SSO, RRH, HP		ES, non-HUD SSO		Outreach	
Data Element	**Missing**	**Don't Know or Refuse**	**Missing**	**Don't Know or Refuse**	**Missing**	**Don't Know or Refuse**
First & Last Name	0%	0%	0%	0%	0%	0%
SSN	0%	5%	0%	5%	0%	5%
Date of Birth	0%	2%	0%	2%	0%	5%
Race	5%	5%	5%	5%	10%	10%
Ethnicity	5%	5%	5%	5%	10%	10%
Gender	5%	5%	5%	5%	10%	10%
Veteran Status	5%	5%	5%	5%	10%	10%
Disabling Condition	5%	5%	5%	5%	10%	10%
Residence Prior to Entry	5%	5%	5%	5%	10%	10%
Zip of Last Perm. Address	5%	5%	5%	5%	10%	10%
Housing Status (Entry)	0%	5%	0%	5%	10%	10%
Housing Status (Exit)	0%	5%	0%	5%	10%	10%
Income & Benefits (Entry)	0%	5%	0%	5%	10%	10%
Income & Benefits (Exit)	0%	5%	0%	5%	10%	10%
Add'l PDEs (Adults; Entry)	0%	5%	0%	5%	10%	10%
Destination (Exit)	0%	5%	0%	5%	10%	10%

6.2.1 Bed Count

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

Table C

Data Entry Time Frame for Bed Counts	
Program type	**Time frame for 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

6.3 Accuracy
Partner 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 CoC and State of Colorado.

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: DPALs will check accuracy and consistency of data by running quarterly program reports (at minimum), monthly highly encouraged, 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

7. Data Quality Plan §580.37 D 1

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

7.1 DPAL

- Runs and reviews reports such as the APR, Universal Data Quality etc. to include all participating programs
- Compares any missing rates to the data completeness benchmarks
- Improves their data completeness rate or provides explanation before the next month's report.
- 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 PA Executive Director for advisement

Table D		
Agency Administrator Report Expectations		
Report	**If annual number of clients served <=50**	**If annual number of clients served >50**
Run Annual Performance Report (Clarity: [HUDX-227])	Quarterly	Quarterly
If receiving ESG funding: Run CAPER (Clarity: [HUDX-228])	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

7.2 Compliance

7.2.1 Data Timeliness

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

7.2.2 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 Table C)

7.2.3 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. (See Table D).

8. Additional Resources

2020 HMIS Data Standards Manual (October 2019):
https://www.hudexchange.info/resources/documents/HMIS-Data-Standards-Manual.pdf
2020 HMIS Data Standards Data Dictionary Version 1.3 (August 2019):
https://www.hudexchange.info/resources/documents/HMIS-Data-Dictionary.pdf
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
Federal Register Final Rule December 4, 2015 24 CFR Parts 91 and 578:
https://www.hudexchange.info/resources/documents/Defining-Chronically-Homeless-Final-Rule.pdf

Appendices

Documents:

Appendix A - Sanctions for Violations

Appendix B - Email Confidentiality Notice

Action Items:

Appendix C - Security and Privacy Checklist

Appendix D - Acknowledgement of Receipt of HMIS Security, Privacy, and Data Plan

Appendix A. Sanctions for Violations

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

A.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 Participating Agency within a 12 month period.

A.1.1 First Violation

A letter documenting violating event and involved personnel will be sent to DPAL from HMIS Lead and kept on-file with HMIS Lead. DPAL 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.

A.1.2 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 DPAL in question. This training must be attended by all end users, the DPAL, and a member of the Partner Agency's executive team. In organizations where the DPAL is the executive director, the training must be attended by the chair or president of the Partner Agency's Board of Directors.

A.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 Monitoring 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 email

The sanction for a major violation is:

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

A.3 Severe Violations

Severe violations include but are not limited to:

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

The 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 Clarity or participating in HMIS data collection for 60 days. The Partner Agency remains responsible for meeting data quality and other obligations during this 60 day period.

Appendix B. 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 email 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

Appendix C. Security and Privacy Checklist

C.1 Data Collection

- Are you collecting the Universal Data Elements on All clients? (Name, SSN, DOB, Ethnicity, Race, Gender, Veteran Status, Disabling Condition, Residence Prior to Program Entry, and ZIP Code for Last Permanent Address)
- Are you collecting Program Data elements? (All CoC-funded, ESG-funded, and/or APR programs collect the Program Data Elements)
- Are you monitoring Data Quality?
- Have users been trained on how to collect data?

C.2 Privacy Notice Policy

- Does your agency have the HMIS Notice of Privacy Practices posted at every place where intakes occur?
- Is a copy of the Privacy Notice available upon request?
- How many intake locations are within the agency?
- Is the HMIS Notice of Privacy Practices posted on your website?
- What is the version date of the HMIS Notice of Privacy Practices?
- Have all users completed the Privacy Training, and do they have documentation of training?
- Have you encountered a need for the HMIS Notice of Privacy Practices to be provided in other languages or formants? (Braille, audio, or large print)

C.3 User Authorization

- How many users are in your agency?
- Do your users share usernames and/or passwords?
- Do you users keep usernames and/or passwords in public locations?
- Do your users store passwords in their internet browsers?
- Do all users have a signed User Agreement on file?

C.4 Hard Copy and Data Disposal

- Does your agency have procedures in place to protect hard copy Personally Identifiable Information (PII) generated from or for HMIS?
- Are all users trained on how to protect and dispose of hard copy data?
- Do you keep hard copy files in a locked drawer(s) or file cabinet(s)?
- Are the hard copies kept in locked offices?
- What is your disposal policy? (Shredding of paper hard copy, re-formatting of disks,

etc.)
- How is client data generated from HMIS? (Printed screen shots, HMIS client reports, downloaded data into Excel, etc.)

C.5 Physical Access

- Are all HMIS workstation(s) in secure locations or are they occupied at all times if they are in public-accessible locations? (This includes non-HMIS computers if they are networked with HMIS computers)
- Are you utilizing password-protected screensavers?
- Are printers that are used to print hard copies from HMIS in a secure location?
- Are users able to access HMIS from outside the workplace? If so, does your agency have a data access policy?

C.6 Virus Protection

- Are all computers networked?
- Do all of your computers have virus protection with automatic updates? (This includes non-HMIS computers if they are networked with HMIS computers)

C.7 Firewall

- Do you have a firewall on the network and/or workstation(s) to protect HMIS systems from outside intrusions?

C.8 Software Security

- Do all your HMIS workstation(s) have current operations systems and internet browser security? (This includes non-HMIS computers if networked with HMIS computers)

C.9 Client Consent

- Do all households entered into HMIS have signed client consent from on file?
- Where are the HMIS client consent forms kept? (Household paper chart, common storage box/drawer, etc.)

C.10 HMIS Agreements

- Has your agency signed and submitted the Agency Partnership Agreement?
- Is your agency listed on the COHMIS website as a Participating Agency?

C.11 HMIS Barriers

- Does your agency have barriers of challenges to entering HMIS data?
- If so, what are they? (Not having enough time to enter date, staff needs more HMIS training, want to keep existing database and import later into HMIS, etc.)

- Are you concerned about the confidentiality or security of HMIS data?
- Are you aware of Techsoup.org?

Appendix D. 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 Colorado Homeless Management Information System (COHMIS)

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 the 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 the HMIS Lead Agency.

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 annually and it is my responsibility to be aware of and to adhere to the changes in the Plan as they occur.

DPAL Name:

DPAL Agency:

Signature: Date: