COHMIS

STATEWIDE POLICIES AND PROCEDURES

v1.1

Part of the *COHMIS Manual*

The *COHMIS Manual* comprises the policies and procedures and 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 four HUD-designated continuums of care (CoCs). The CoCs maintain the COHMIS to help reduce homelessness in Colorado.

1. HMIS Historical Background

1.1 Definition of Homeless Management Information System (HMIS)

A Homeless Management Information System (HMIS) is a locally administered data collection tool used to collect ongoing longitudinal data on homeless families and individuals—and on persons at risk of becoming homeless—who receive assistance from community homeless and other human services providers. The longitudinal data collected can be used to better understand the size, characteristics, and needs of the population for purposes of grant writing, program evaluation, and advancing effective fact- based funding and legislative decision making.

1.2 HUD HMIS Requirement

In July 2003, the Department of Housing and Urban Development (HUD) published a draft notice of the HMIS Technical Data Standards.[1] In July 2004, HUD finalized this notice and published it in the Federal Register to encourage communities around the nation to set up an HMIS. The notice specified what data elements should be collected and established minimum baseline policies and procedures for privacy, confidentiality, and security standards designed to protect client-level data. In 2005 the Annual Homeless Assessment Report (AHAR) reporting process was established, and in 2018, HUD updated the AHAR into the Longitudinal System Analysis (LSA).[2] This process identifies the procedures for collecting and reporting HMIS data to Congress for use in making federal appropriation decisions. During the same time-period, HUD informed communities that HMIS data collection would be given points in the Super NOFA grant application ratings. The vision was that as communities participated in HMIS, more accurate information would be collected. This information would be more reflective of the plight of the homeless and at-risk populations, resulting in a better, national understanding. In 2018, HUD amended the HMIS data standards.[3] HMIS databases are the de-facto databases used for HUD-sponsored homeless and at-risk data collection efforts. As the standards continue to evolve they will produce data that can positively impact policy decisions that address the problem of homelessness in the United States.

1.2.1 The HEARTH Act

The HEARTH Act, enacted into law on May 20, 2009, requires that all communities have an HMIS with the capacity to collect unduplicated counts of individuals and families experiencing homelessness. Through their HMIS, communities should be able to collect information from projects serving homeless families and individuals to use as part of their needs analyses and to establish funding priorities. The Act also codified into law certain data collection requirements

[1] https://www.hudexchange.info/resources/documents/2004HUDDataandTechnicalStandards.pdf
[2] https://www.hudexchange.info/homelessness-assistance/LSA/
[3] https://www.hudexchange.info/resources/documents/HMIS-Data-Standards-Manual.pdf

integral to HMIS. With enactment of the HEARTH Act, HMIS participation became a statutory requirement for recipients and subrecipients of CoC Program and Emergency Solutions Grants (ESG) funds.[4]

1.3 Applicable Laws or Regulations Affecting the System

1.3.1 The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

HIPAA's Privacy Rule states that "Individually Identifiable Health Information" is to be considered "protected health information" [PHI] subject to the review and control of individual patients. Agencies and other entities handling PHI are mandated to restrict access to such information to appropriate persons and protect the privacy of individuals. Clarity HMIS includes customization features at micro and macro levels to automate the enforcement of federal, state, and local privacy requirements such as HIPAA. Clarity HMIS Security Tools enable each partner agency to define which client data is shared with other agencies at every level, including the field level.

1.3.2 HB18-1128 Protections For Consumer Data Privacy

Except for conduct in compliance with applicable federal, state, or local law, the bill requires covered and governmental entities in Colorado that maintain paper or electronic documents (documents) that contain personal identifying information (personal information) to develop and maintain a written policy for the destruction and proper disposal of those documents. Entities that maintain, own, or license personal information, including those that use a nonaffiliated third party as a service provider, shall implement and maintain reasonable security procedures for the personal information. The notification laws governing disclosure of unauthorized acquisitions of unencrypted and encrypted computerized data are expanded to specify who must be notified following such unauthorized acquisition and what must be included in such notification.

More info on the bill can be found at https://leg.colorado.gov/bills/hb18-1128.

1.4 Vision for HMIS

The vision for this system within our State is to exceed HUD's reporting expectations. Our vision is that clients, agencies, and the community benefit from a streamlined approach to referrals, intakes, and assessments across the entire service delivery system. We envision that our Statewide HMIS will offer the following benefits:

- Ensuring that each CoC's Lead Agency is in regulatory compliance with HEARTH Act and HUD system requirements as outlined in current HUD Data Technical Standards.
- Coordinated case management across agencies, programs, and services that is designed to achieve a one-stop-shop concept

[4] https://www.hudexchange.info/programs/hmis/hmis-requirements/

- The ability to track and measure outcomes achieved by the four Continuums of Care (CoC) and other programs within the CoCs
- Service coordination within communities with a goal of moving towards statewide service coordination
- More information shared with funders, boards, and other stakeholders that can be used to inform and facilitate data-driven decisions
- An improved understanding of the problems, issues, and needs of persons experiencing homelessness and at-risk populations
- The development or modification of state and local policies that can identify or reduce service gaps and help end homelessness
- The ability to track and measure outcomes for the goals outlined in federal, state and local plans to end homelessness.

2. Colorado's HMIS Structure

Colorado's HMIS Statewide Collaborative is a group representing the four HUD Continuums of Care: Metro Denver Homeless Initiative (MDHI), Pikes Peak, Balance of State, and Northern Colorado

Colorado CoC:	**MDHI**	**Pikes Peak**	**Balance of State**	**Northern Colorado**
Address:	711 Park Ave West Suite 320 Denver, CO 80205	121 S Tejon Street Suite 601 Colorado Springs, CO 80903	2111 Champa Street Denver, CO 80205	242 Conifer Street Fort Collins, CO 80524
Executive Director:	Matthew Meyer	Amber Ptak (Interim CEO)	John Parvensky	David Rout
HMIS Lead Agency Contact:	Kyla Moe	Michelle Whiting	Denny Wetmore	Marla Sutherland

The Collaborative is responsible for providing counsel and assistance to the HMIS Lead Agencies, staff members, CoC governing bodies, and contributing providers within each of the four participating CoC on all matters regarding homeless service data and HMIS. For more information please refer to the updated COHMIS Statewide Collaborative Governance Framework.

3. Implementing HMIS

3.1 Agency Partnership Agreements

To use the HMIS, an agency must sign and agree to abide by the terms of the COHMIS Agency Partnership Agreement. The Agency Partnership Agreement is between the agency and the

HMIS Lead Agency as designated by the CoC. Agencies that provide services in multiple CoC's must sign an Agency Partnership Agreement with the HMIS Lead in their respective CoC's. The Agency Partnership Agreement details participation guidelines and policies and procedures that must be followed in order to use the HMIS provided by Bitfocus for Colorado's CoCs. The agreement outlines steps that must be taken to protect client data and ensure that all information is collected and entered in a timely manner with good data quality and completeness. It also defines requirements pertaining to confidentiality, data entry, roles and responsibilities, security, reporting, and other items deemed necessary for proper HMIS use and operation.

Procedure for completing the Agency Partnership Agreement:

1. Download the Agency Partnership Agreement from the COHMIS website.
2. Review and execute the Agency Partnership Agreement.
3. Designate a Data Partner Agency Liaison (DPAL) to work between the Partner Agency and the HMIS Lead Agency
4. Submit a ticket to the COHMIS Help Desk to your CoC with the executed Agency Partnership Agreement and the contact info for the DPAL.

3.2 Designate Data Partner Agency Liaison

Data Partner Agency Liaisons (DPALs) play an important role in communicating and leading the effectiveness of HMIS at a Partner Agency-level. The DPAL is the central point in the Partnership Agency Agreement facilitating communication between their Agency Staff and the HMIS Lead Agency. The DPAL must be an active user and will be the first point of contact within their respective agencies for HMIS issues and questions.

Agencies may also request support from the Lead Agency with report generation and new user access, if they do not have an assigned DPAL. The DPAL helps support the included, but not limited to:

- Authorize End Users and access levels
- Request changes to end user access levels
- Report incidents and breaches related to privacy or security
- Oversee internal HMIS monitoring
- Runs and reviews internal performance and Data Quality reports regularly
- Answer end user questions about HMIS database
- Act as an HMIS expert for the Partner Agency and promote use of HMIS data within the agency.

An overview of the DPAL role is available in the COHMIS DPAL Agreement.

3.3 Technological Requirements for Participation

Operating System	Windows 7+/Mac OSX 10.5+
Processor Speeds	Intel or ADM Dual Core
RAM	2 GB RAM
Connectivity	Cable or ISDN (Minimum 256 kbps/user)
Firewalls	Yes
Routers	Yes
Supporting Software	Firefox, Explorer, Safari, Chrome, Microsoft Edge

3.4 Agency Profiles

Each agency must be set-up in HMIS, and profiles that define the programs and services the agency offers must be completed prior to HMIS use and data entry. Agencies cannot use HMIS until the Agency Profile sheets have been verified and approved by the CoC's Lead Agency. Agency Profiles will be reviewed by agencies and updated on an annual basis as necessary.

Agency profile completion procedures:

1. Agencies should contact the relevant CoC HMIS Helpdesk to obtain a copy of the Agency Profile Worksheets.
2. The Helpdesk can provide recommendations and assistance with completing the Profile Worksheets.
3. It's the agency's responsibility to ensure that their Agency Profile Worksheet programs and services are consistent with grant requirements and to update the Lead Agency with any changes.
4. All completed Profile Worksheets must be emailed to the CoC HMIS Helpdesk. Once received the CoC Helpdesk administrators will work with the agency's Site Administrator or relevant staff member to review the profile worksheets. In order to ensure accurate set and reporting, the worksheets must reflect the agency/grant requirements and the programs and services must be organized in effective and efficient manner that promotes CoC consistency, best practices and efficient data usage as determined by the CoC Lead Agency.

4. User Administration

4.1 Authorizing Personnel for HMIS

Only authorized individuals who have successfully completed the necessary training and have signed and submitted the COHMIS End User Agreement will be allowed to access HMIS on behalf of their agency. Partner Agencies are responsible for providing basic confidentiality

training to all staff, volunteers and other persons issued User IDs and passwords for HMIS. HMIS End User training will review confidentiality and security elements prior to authorizing access. Partner Agencies shall refer to their personnel policies, current HMIS Policies and Procedures, and current HUD Data and Technical Standards to determine if their staff, volunteers and other persons should be issued unique User IDs and passwords.

The Agency DPAL can pull a report at any time, reflecting a current list that identifies all authorized users and their assigned access level(s) and activity.

4.2 Designating End Users

Any individual working on behalf of the agency (employee, contractor, and volunteer) that will collect information for HMIS purposes must be designated as an HMIS end user, and therefore is responsible for adhering to the policies and procedures set forth in the manual. Anybody who collects any HMIS data (electronic or paper) or creates reports from the system is deemed an HMIS end user. HMIS end users are held accountable for the custody of client level data and for the privacy, confidentiality, and security of that data.

Without the proper training, individuals will not be prepared to respond to clients' questions regarding HMIS consent, revocation, intake forms, and other aspects of HMIS data collection. In order to designate an HMIS user, the end user will complete required end user trainings and pass all testing elements. During this training process, end users will request end user access from their agency DPAL who will submit their request to the HMIS Lead Agency. It is in the best interest of agencies to have several employees trained and credentialed; this strategy is good for backup purposes and enables employees within the agencies to help each other and assist with client questions and/or concerns.

4.3 End User Agreements

The End User Agreement is a contract between a Partner Agency and its employees, contractors, or volunteers who are authorized to collect HMIS data and/or enter data into the system as end users. All end users must sign the agreement stating that they will abide by the policies and procedures associated with protecting the privacy, confidentiality, and security of client level data. End users will be required to keep updated End User Agreement Forms annually within the Clarity system. The HMIS Lead Agency should never delete a signed COHMIS

End User Agreement upon revoking an individual's authorization or in terminating an individual's employment.

4.4 Assigning Security Levels

HMIS Lead Agency staff will work with Partner Agencies to ensure that end users are assigned the appropriate security level and have appropriate access to libraries based on their role. Within HMIS, each end user is assigned a role that is associated with a certain level of security. This security allows users to gain access to certain areas of the HMIS application. End user security is utilized to ensure that individuals can only access the type of client level information necessary to do their job. An example would be that an intake specialist would be assigned

access to general information which would enable them to view basic client demographic information (name, birth date, ethnicity, etc.); however, their security role would not allow them to pull agency-wide reports on clients enrolled in programs.

The three end user roles available are:

- Basic – this role is the most frequently assigned offering access to Clarity for the main HMIS functions. Specific access to functions within HMIS (e.g. program enrollment reports, etc.) will be based on need and the roles of staff.
- Manager – this role is limited to fewer staff at each agency and could include the DPAL, and offers everything the Basic role provides, plus enhanced reporting.
- System Administrator – this role is reserved for HMIS Lead Agency staff, as they offer full system access.

Procedures for determining appropriate access:

1. COHMIS Helpdesk personnel will grant individuals access to the appropriate libraries and pages based on the agency's description of each user's role. To assign the security level for a user the agency should submit an End-User Account Request Form to the COHMIS Helpdesk. Please ensure that an updated list of approved users has been submitted.
2. Agencies may contact the COHMIS Helpdesk if it is determined that an end user may need a different type of access in HMIS. All requests for permissions changes will be handled on a case-by-case basis. The COHMIS Helpdesk will work diligently with agencies to ensure all end users have proper permissions in HMIS by examining the end user's role.

4.5 Changing Personnel Security Levels

To request a change to an employee's access level (e.g. from End User to Manager access), DPALs should submit a ticket to their CoC Help Desk indicating the user accounts needing change. License types and quantities are limited based on Partner Agency and availability across the CoC, so not all requests may be confirmed depending on availability.

4.6 Removing Authorized Personnel

The COHMIS Helpdesk must be notified within one business day when an individual is no longer authorized to access HMIS on the agency's behalf. The DPAL should submit a ticket to their CoC Help Desk indicating the user account needing deactivation. Upon receipt of the request, the HMIS Lead Agency will immediately deactivate the individual's HMIS user account. The HMIS Lead Agency should never delete end user accounts in order to provide a record of all end users with access historically, and instead should deactivate accounts accordingly.

All end user accounts are subject to a 90-day activity review, with a 15-day warning; if an end user does not login to HMIS within a 90-day period, their access will be deactivated

automatically. This access can be reactivated by the DPAL submitting a ticket to the CoC Help Desk indicating the user account needing reactivation, along with a reason as to why the end user had not logged in within 90 days and still needs access. And end user who has been deactivated for six months or more must work with the Lead Agency to be re-authorized, which could include additional training.

4.7 Deactivation Due to Incompletion of Refresher Trainings

Each year, users must complete a refresher training to ensure continued understanding of HMIS. If a user does not complete this training by the quiz deadline, their access to HMIS will be deactivated until the respective CoC Lead Agency's Help Desk confirms that the user has taken, and passed, this quiz. Once confirmed, the user's access to HMIS will be reinstated.

5. Training

5.1 First-time Access to HMIS

End users must complete two trainings, HMIS 101 & HMIS 201, to gain initial access to the Clarity HMIS system.

5.1.1 HMIS 101 Training

1. After an individual is identified as a possible HMIS end user, the end user is directed to watch the pre-recorded CO HMIS 101 Training Videos posted on the Statewide Colorado HMIS website, which provide an overview on the basics of HMIS, policies and procedures, data quality, data standards, data collection, and any CoC specific messaging as needed. A link to the training website can be found here:
2. The end user reviews the HMIS 101 Training Videos and notifies their agency's DPAL, who sends authorization to their HMIS Lead Agency.
3. The HMIS Lead Agency distributes the link to the online HMIS 101 quiz to the end user. End users will be allowed to take the quiz more than once if necessary.
4. End users that score 80% or higher are then considered to have passed HMIS 101 Training and proceed to the HMIS 201 Training.

5.1.2 HMIS 201 Training

1. The CoC HMIS Lead Agency sends a registration link to the end user for the next available HMIS 201 end user training, which is a more hands-on walkthrough of entering client data into Clarity.
2. After the end users completes HMIS 201 training, the CoC HMIS Lead Agency will then setup the end user in Clarity, distributing the username and temporary password to the end user.

3. The end user logs in to Clarity for the first time using the login information provided from the CoC HMIS Lead Agency, at which time the end user will be prompted to digitally sign their HMIS End User Agreement within Clarity and change their temporary password.

5.2 HMIS Basics

5.2.1 System Idle Times

If the user is inactive (idle) for 30 minutes, the system will log the user out. At 25 minutes of idle time, the user will receive an on-screen warning that their session will end in 5 minutes. A pop-up will appear, and if the user is still using the system, they may select the appropriate button to continue their session.

5.2.2 Passwords and Lockout Times

Passwords should be unique and should never contain personal identifying information, such as the user's name. The system will require users to choose a certain format for passwords (e.g. upper and lower case letters, numbers, symbols, etc.)

If a user enters their password incorrectly 4 times, they will be locked out of the system for 1 hour. This is a security measure designed to protect both users and the sensitive data that the system contains. To avoid waiting, users may email the COHMIS Helpdesk to request a password reset. Upon receiving a temporary password, the user **must** create a new password when first logging into the system**.**

Users will be required to change their password every 90 days. At 75 days, users will receive a notice to reset their password in 15 days. Users may reset their passwords when notified on the 75th day if they choose. The password reset date then resets to 90 days.

Storing passwords in internet browsers **is prohibited**.

6. Data Collection

6.1 On Whom To Collect Data

Agencies should attempt to collect data from families and individuals who are homeless or at risk of becoming homeless and are accessing services from their agency. Each program within an agency should strive to collect information from consenting adults and household members who will benefit from the services rendered. Agencies should strive to collect information to accurately portray who they helped. This information can be used to fulfill funder reporting requirements and to produce agency/community statistics for planning purposes. It is important for agencies, especially emergency services providers, to know basic information about clients who are served, their household composition and services provided. Agencies may also choose to collect data for HMIS on individuals or families that make contact with the agency but are not able to receive services from the agency. One of the greatest benefits of

HMIS to an agency is its ability to create reports describing the agency's clients, outcomes of the services they receive, and general agency operating information.

Procedures:

1. For HMIS purposes, HUD's minimum standards require that individuals or families who are homeless or at risk of becoming homeless and are accessing services from an agency must be approached for HMIS data collection. However, some programs/agencies may Require HMIS participation. See link:
https://www.hudexchange.info/resources/documents/HMIS-Data-Standards-Manual.pdf
2. During the intake process, it is important to identify those persons who meet the HUD standards. Once these persons are identified, they must give their consent to HMIS data collection through implied consent (posted), verbal consent or informed (written) consent.
3. Clients can choose not to participate in HMIS unless it is a condition of program enrollment.
4. Information must be collected on each family member, not just on the head of the household.

6.2 Client Consent and HMIS Participation

Agencies must decide for each of their programs whether to obtain consent through implied (posted privacy notice), verbal, or informed (written authorization) methods. Regardless of the type of consent method used, all consent must be obtained fairly and in good faith. The HUD HMIS Data and Technical Standards[5] allow agencies to collect data using implied consent at minimum, given that some agencies service a high volume of clients. The standards also recognize that there may be a need for greater privacy protection and recommend informed consent in those cases. The three forms of consent are defined briefly below.

- Written consent: The client signs a form to agree/disagree to participate in HMIS data collection.
- Implied consent (posted privacy notice): HMIS data collection is explained and the client gives their information freely, without directly being asked to participate.
- Verbal consent: The client verbally agrees/disagrees to participate in HMIS data collection.

[5] https://www.hudexchange.info/resources/documents/HMIS-Data-Standards-Manual.pdf

Agencies can decide by program how to obtain consent based on what is the most practical method for the program type (e.g., verbal consent for call-based referrals versus informed consent for housing programs). Consent must be obtained in a consistent manner within each program, meaning that all program's clients must provide the same form of consent. Agencies

that serve non-English speaking clients should provide consent information in a language that their clients can understand (e.g., Spanish).

When an individual decides not to participate in HMIS, an agency cannot deny them services solely for that reason. However, agencies may need information from the client in order to provide services (for example, social security number needed to secure TANF benefits). In examples like this, agencies are not required to guarantee services. Agencies should determine if an individual will or will not receive services before the individual goes through the informed consent process. This will eliminate a perceived relationship between HMIS participation and service delivery.

Procedures:

1. Agencies must formally decide by program which method will be used to obtain client consent. Agencies shall identify which method(s) they are using on the Agency Partnership Agreement and submit changes in writing to the HMIS Lead Agency.
2. Each program must consistently use the same method for obtaining consent.
3. Agencies will follow HUD's minimum guidelines for achieving implied consent.
4. Only an authorized HMIS end user who has completed the HMIS Policies and Procedures Training may obtain consent from clients.
5. HMIS users must obtain consent from clients in a manner that is respectful, fair, and in good faith for both the client and HMIS (meaning that the explanation of HMIS, data collection, client rights, etc., must be provided in an objective manner).
6. The HMIS user must adhere to the agency's decision for the applicable program regarding the method of obtaining consent.

6.2.1 Implied Consent Posted Privacy Notice

The COHMIS Implied Consent Posted Privacy Notice is a brief document that describes a consumer's rights in relation to HMIS and identifies other agencies that have access to HMIS data. These notices must be appropriately posted within an agency and are available on the COHMIS website. An agency could also post the Implied Consent Posted Privacy Notice in waiting rooms, adjacent to intake lines, or in other areas where clients congregate before intake occurs. This will give clients an opportunity to read the notice before receiving services.

Procedure:

1. Implied consent notices must be posted anywhere client level data is collected.
2. Each workstation, desk, or area that is used during HMIS data collection must post the COHMIS Implied Consent Posted Privacy Notice.
3. If an individual or family does not speak English, the agency must attempt to obtain consent to the best of their abilities in a language the client understands. COHMIS forms are currently available in English and Spanish. Other reasonable accommodations, such as languages or mediums of communication (e.g. Braille, TTY, etc.), must be made

available to clients based on their cultural and linguistically appropriate needs.

6.2.2 Verbal Consent and HMIS Participation

Verbal consent is obtained by delivering to the client an agreed-upon agency script that provides an explanation of HMIS. The script details why HMIS data is being requested and outlines the client's rights related to HMIS data collection. All employees working with clients should consistently use the script to collect client level HMIS data. Agencies that decide that their program will collect verbal consents should contact their HMIS Lead Agency for a sample script.

6.2.3 Written Consent and HMIS Participation

Agencies that decide that their program will collect written consent should use the standard COHMIS Client Consent for Data Collection and Release of Information form. Agencies should start with this standard form and add any additional information as necessary. A verbal explanation should be given to the client to inform them of the necessity and importance of collecting their data prior to having the client sign the consent form. Agency staff should review the consent form with the client to ensure that it was filled out appropriately, and then sign as a witness.

Procedures:

- Agency staff should use a verbal script similar to that used for verbal consents, to explain the HMIS security and privacy policy.

6.3 RHY (Runaway and Homeless Youth) Programs

- Data may not be shared about any youth served in a RHY-funded program unless the youth has consented.
- Youth under the age of 18 in a RHY-funded program must receive the required parental consent prior to the sharing of their information.
- Youth age 18 or over may consent for themselves.[6]

[6] https://www.rhyttac.net/index.php?option=com_content&view=article&id=177:rhy-data-sharing-and-data-transfer-for-local-hmis&catid=26:rhy-news&Itemid=211

6.3.1 Non-RHY Programs

- Unaccompanied youth who are at least 15 years old can give their consent to the collection of information about them, even when consent has not been obtained from their parent or guardian.
- Parental/guardian consent can override the youth's consent up to age 18.
- The consent of an unaccompanied youth under the age of 15 can be provided only by their parent or guardian.

6.4 Prioritization of Chronically Homeless Clients and Recordkeeping

Agencies must abide by the HUD *Notice on Prioritizing Persons Experiencing Chronic Homelessness and Other Vulnerable Homeless Persons in Permanent Supportive Housing and Recordkeeping Requirements for Documenting Chronic Homeless Status.*[7] This applies to both the prioritization of clients by vulnerability and the recordkeeping requirements.

6.5 Presumptions of Competency

Clients are presumed to be competent to provide consent, unless there is a known court order claiming their inability to make informed decisions.

Procedure:

1. If there is a known court order stating that the individual is not competent to make informed decisions, then it will not be possible to obtain informed consent for HMIS participation. In this case, the HMIS user should treat this client as a non- participant.
2. HMIS users should do their best to obtain informed consent from individuals for whom there is no court order, but who appear to be not fully competent during intake. If it is not possible to obtain a truly informed decision regarding HMIS participation, the individual should be dealt with as a non-participant.
3. Often individuals may have temporary limits on their competency because they are under the influence of a particular substance, which affects their ability to make a decision. If it is possible, delay the informed consent and HMIS data collection until they are no longer under the influence and are able to make decisions.

6.6 Client Access to Information Collected

Clients have the right to a copy of the data collected from them in HMIS. Agencies are required to print out this information for any client who requests it. If an agency uses hard copy forms to collect the data then a copy of the form can be given to the client.

[7] https://www.hudexchange.info/resource/5108/notice-cpd-16-11-prioritizing-persons-experiencing-chronic-homelessness-and-other-vulnerable-homeless-persons-in-psh/

Agencies are not required to provide any additional information from HMIS to clients (i.e., data that was not collected directly from the client, such as case notes). Disclosure of such information is left to the discretion of the agency.

Procedure:

1. If paper forms are used to collect data from clients, with data entry into HMIS occurring later, consider making a photocopy of the paper forms for the client if they request a copy of the data they provided.
2. Agencies may give clients a copy of the Posted Privacy Notice or Client Informed Consent form, which notify clients of their rights.
3. Agencies that request informed consents may also wish to provide clients with a photocopy of their consent signature page so that the client has a record of their HMIS participation decision.
4. Case management notes are typically not shared with the client. However, elements of case plans such as their Goals, Outcomes, Referrals, and Services can be provided.

6.7 Storing Informed Consent Forms

Informed consent forms should be stored securely in the Clarity database instance, either as a digital signature or a scanned document file. It is important that informed consent forms be kept for at least seven years of time for auditing purposes.

Procedure:

1. Informed consent forms must be kept securely in the Clarity instance (preferred) or in accordance with standard confidentiality and privacy practices for physical files (i.e., locked away in a file cabinet and not accessible without authorization).
2. It is recommended that agencies store informed consent forms in their client files rather than creating a separate file just for HMIS, unless client files are purged prior to seven years after the client last receives services.

6.8 Using Paper-Based Data Collection Forms

Each agency must determine how best to incorporate HMIS into their operating processes. Digital submission and recordkeeping is preferred. Agencies may choose to collect client level data on paper prior to entering the data into HMIS. When this process is used all of the data gathered on the forms must be entered into the database within a timely manner as listed in the COHMIS Security, Privacy and Data Quality Manual. It is preferable to enter data directly into HMIS as it is collected rather than first recording it on paper. Whether direct data entry or

paper forms are used the data collected and entered must be consistent with that specified on the hard copy forms provided by COHMIS. COHMIS uses four sets of forms for HMIS data collection: Universal Intake, Program-Specific Intake, Interim Assessment, and Exit/Discharge. The appropriate forms to use are based on program type as specified in the COHMIS Security, Privacy and Data Quality Manual. Typically, all programs use the Universal Intake forms, while programs that prepare Annual Progress Reports or other reporting required by funders must also use the Program-Specific Intake form. Programs that produce Annual Progress Reports are also required to use the Interim Assessment form for annual evaluations. If a Participating Agency has questions regarding which forms to use, they should contact their HMIS Lead Agency for assistance.

The HMIS forms used by COHMIS are:

- Universal Intake Form:
    - Head of Household Intake Form
    - Other Household Member Intake form (When information is being collected on a family, it must be collected on each and every member of the family.)
- Program Specific Intake Form
- Interim Assessment Form
- Exit/Discharge Form

Procedure:

1. Agencies may utilize paper-based forms for data collection, but digital recordkeeping is preferred wherever possible.
2. When paper forms are used, the data collected must be entered into HMIS within a timely manner as indicated in the COHMIS Security, Privacy and Data Quality Manual.
3. The Universal and Program-Specific intake forms can be obtained from the COHMIS website. Agencies receiving funds from Federal homeless assistance grants are required to utilize the Program-Specific forms, Interim Assessment form and Exit/Discharge form. Agencies not receiving these types of funds may choose to use the Universal forms.
4. Agencies that are not required to use the Program-Specific Intake form are urged to collect this data anyway, depending upon the type of programs and services the agency offers. The additional data can prove extremely helpful for internal and external reporting on client outcomes and services delivered.
5. Agencies that wish to customize CoC data collection forms to include their own required fields should contact their CoC HMIS Lead Agency for assistance to ensure that minimum data collection standards are met.

6.9 Collecting Client Disability Information

Under the data standards required by HUD, agencies must ask clients questions about disabilities. To comply with other federal laws and regulations, these client questions must be asked at a certain point in time. HUD defines 'disabling condition' as: “(1) a disability as defined in Section 223 of the Social Security Act; (2) a physical, mental, or emotional impairment which is (a) expected to be of long-continued and indefinite duration, (b) substantially impedes individual's ability to live independently, and (c) of such a nature that such ability could be improved by more suitable housing conditions; (3) a developmental disability as defined in section 102 of the Developmental Disabilities Assistance and Bill of Rights Act; (4) the disease of acquired immunodeficiency syndrome or any conditions arising from the etiological agency for acquired immunodeficiency syndrome; or (5) a diagnosable substance abuse disorder.

6.10 HMIS Data Collection Standards

COHMIS has developed standardized data collection instruments for participating agencies to enable effective and efficient analysis of collected data listed in the COHMIS Security, Privacy and Data Quality Manual. It is important to standardize the data by program type as the goal is to use this data to make informed decisions.

6.10.1 Programs that are not required to report program-specific data to HUD

Universal Data Elements: HUD requires all agencies participating in HMIS to collect a standard set of client information, known as the Universal Data Standard, as well as any additional “community reporting” data required by the CoC. Examples of the Universal data elements, which are specified on the Universal Intake forms described in section 6.7, include the following: name, social security number, birth date, ethnicity, and race. Additional data required by the CoC include the responses to such questions as “Are you homeless?” and “How many times have you been homeless in the last three years?”

6.10.2 All housing programs (S+C, SSO, SRO, ESG-RR/HP, Transitional, Permanent and Permanent Supportive Housing programs) that are required to report program-specific data to HUD through Annual Progress Reports

Program Specific Data Elements: Programs receiving funding from federal homeless assistance grants are required to collect the data elements specified in HUD's Program-Specific Data Standard. Examples of the Program-Specific fields include: income, education, employment, military service, and health.

6.10.3 Emergency Solutions Grant (ESG) and Service Only programs that are not required to report program-specific data to HUD through Annual Progress Reports

ESG Data Elements: These programs are required to collect the data elements specified in HUD's ESG Data Standard. Examples of the ESG data include: income, military service, and health.

6.11 Sharing Client Data

HMIS client data will be shared in accordance with the Agency Partnership Agreements. Sharing enables agencies that work together to coordinate their service offerings and work toward the objective of ending homelessness. COHMIS allows groups of agencies to share the same client record. With the implementation of coordinate entry, sharing client level information will be an integral part of successful assessment, prioritization, referral and housing placement. When coordinating services, it is important to keep the client's Personally Identifiable Information (PII) confidential, unless the client expressly permits that information to be shared. Agencies that wish to have the ability to share records with one another will need to sign the Sharing Business Associates Agreement. Clients will also have the ability to decide if they want their information shared, unless the program/agency collecting their data requires data sharing.
HMIS end users should maintain the highest levels of privacy and confidentiality at all times and must not disclose personal identifiable information except when it is necessary.

6.11.1 Sharing Thresholds

Full Shared. Shared between, and editable by, all participating agencies. Other agencies will have full access to view all information on the client's profile screen.

- Client intake record: Name, birth date, SSN, gender, race, ethnicity
- Household and contact information: Household name, household relationships, household address
- Client photo
- Public Alerts (agencies have the ability to restrict alerts to their agency only)

Basic Shared. Other agencies will see that service, program and assessments transactions have occurred, and view the details of these transactions.

- Program enrollments: case name, entry/exit dates, program name, program type, organization name
- Services
- General client assessment data: income, general health, education, etc.
- VI-SPDAT assessments
- Client Files
- Client Forms

Not Shared. Limited to the organization that created the record.

- Sensitive client data: case notes, HIV/AIDS status, mental illness, domestic violence, alcohol abuse, substance abuse
- Client notes
- GPS locations

Sharing of youth data:

- Youth under the age of 18 must have parental consent to have their data shared.[8]

6.12 Filing a Grievance

Clients have the right to file a grievance if they feel their privacy rights have been violated. If a client files a grievance against an agency, the HMIS Lead Agency will ensure that there is no retaliation taken against the client.

Procedure:

1. The client must request and complete the grievance form used by the agency.
2. The client may provide the form to a Partner Agency manager, DPAL or another person of authority not related to the grievance OR may mail the form to their HMIS Lead Agency contact.
3. When a Partner Agency receives a completed grievance form, it must submit the form to the HMIS Lead Agency within two business days.
4. The HMIS Lead Agency will review the grievance, research the nature of the complaint, and respond to the individual filing the grievance with a copy going to the Partner Agency within 30 days.
5. The Partner Agency named in the grievance may not refuse or reduce services to the client because of the filing of a grievance.
6. If a client reports retaliation due to filing a grievance, the retaliation will be investigated by the CoC's Board of Directors.

6.13 Revoking Authorization for HMIS Data Collection and Sharing

Clients who initially agree to participate in COHMIS have the right to rescind their permission for data collection and sharing.

Procedure:

1. Clients must request and complete the COHMIS Revocation Form and submit it to the Partner Agency.
2. The Partner Agency will submit the revocation form to their HMIS Lead Agency.
3. The HMIS Lead Agency will process the request and confirm with the Partner Agency and client the revocation process date.
4. The HMIS Lead Agency will review the client history and inform all agencies who have worked in the client file that the client record will be de-identified. The HMIS Lead Agency will provide the unique ID to each agency so they may access the client's record, if needed.

[8] https://www.rhyttac.net/index.php?option=com_content&view=article&id=177:rhy-data-sharing-and-data-transfer-for-local-hmis&catid=26:rhy-news&Itemid=211

6.14 Reducing Duplicate Records in HMIS

To avoid creating multiple records for the same client within HMIS, HMIS users must always search to see if a record already exists for the client before creating a new client record.

Procedure:

1. When an HMIS user is collecting data from an individual or family, the user must search within HMIS to determine whether a client record already exists in the system before establishing a new record.
2. Since abbreviated names (such as Ken instead of Kenneth) are sometimes used, or misspellings are made, Users must search using the first three letters of the client's first name and last name and/or the last 4 digits of the SSN. Searching by date of birth (DOB), is helpful as well.
3. If a record corresponding to the person does not exist, then the HMIS User must create a new client record.
4. If duplicate records are found, alert the HMIS Lead Agency for record merging. Always email client IDs only, without PII.

6.15 Client Discharge – Completing Required Fields for HMIS

When a client is being discharged or is exiting the program, HMIS users must ensure that all Universal and CoC-required data fields have been completed, and that any required Program-Specific data fields have been completed, within the client's HMIS record. See sections 6.7 and 6.9, above, and the COHMIS Security, Privacy and Data Quality Manual for more information on these data fields.

7. HMIS Quality Assurance

7.1 What is Data Quality?

Data quality refers to the reliability and validity of the client level data collected in HMIS. It is measured by the extent to which the client data in the system reflects actual information in the real world. More specifically, the quality of data is determined by assessing its timeliness, completeness, and accuracy. For specific information on Data quality requirements, please review the COHMIS Security, Privacy and Data Quality Manual.

- Timeliness—Entering data in a timely manner can reduce human error that occurs when too much time has elapsed between the data collection (or service transaction) and the data entry. The individual doing the data entry may be relying on handwritten notes or their own recall of a case management session, a service transaction, or a program exit date; therefore, the sooner the data is entered, the better are its chances of being correct. Timely data entry also ensures that the data is accessible when it is needed,

either proactively (e.g., for monitoring, increasing awareness, or meeting funding requirements) or reactively (e.g., for responding to requests for information).

- Completeness—Partially complete or missing data (e.g., an incomplete SSN, a date of birth without the year, missing information on disability or veteran status) can negatively affect an agency's ability to provide comprehensive care to clients. Missing data could mean that the client does not receive needed services that would have been prompted by complete data—services that could help the client become permanently housed and no longer homeless.
- Accuracy—It can be difficult to assess the accuracy of HMIS data. It depends both on the client's ability to provide correct data and the intake worker's ability to document and enter the data accurately. Consistency directly affects the accuracy of data; if an end user collects all of the data, but doesn't collect it in a consistent manner, then the data may not be accurate. Accuracy will be assessed based on the monitoring activities outlined in the COHMIS Security, Privacy and Data Quality Manual.

7.2 HMIS Data Quality

HMIS users are required to ensure the quality of the information that they enter into HMIS, as stated in the End User Agreement and the Data Quality Plan. There are several reasons why data quality is important to everyone, from clients to users to agencies to the community. If information is not collected accurately, clients may experience issues trying to coordinate multiple service providers, receiving appropriate referrals, and determining their eligibility for services. HMIS users may have trouble serving clients appropriately without accurate information being collected and maintained. Agencies and the community will face reporting and decision-making challenges without accurate data.

Procedure:

1. HMIS users will assess the completeness and accuracy of the data gathered from clients as it is collected and entered into HMIS.
2. DPALs will review data quality on a recurring basis and use their findings to address corrections or concerns.

7.3 Data Quality and Correction

The DPAL or their designees are required to facilitate the correction of data quality problems identified on data quality reports. The HMIS Lead Agency will work with the DPAL to support them in ensuring that the data contained within HMIS is of high quality. Information about the data quality reports required by the CoC can be found in the COHMIS Security, Privacy and Data Quality Manual.

7.4 Ensuring Data Quality across the CoC

Unresolved data quality issues will be subject to corrective action as described in the COHMIS Security, Privacy and Data Quality Manual.

8. COHMIS Help Desk Procedures

8.1 Data Partner Agency Liaison

DPAL should provide the first level of technical assistance for Partner Agency HMIS end users. The DPAL should be the best resource for information about the agency's policies and procedures as they relate to HMIS. If the DPAL is unable to resolve any HMIS user concerns they will contact their HMIS Lead Agency for assistance.

8.2 Contacting COHMIS Helpdesk

COHMIS users can find a wealth of information on the COHMIS Help Desk Portal: cohmis.zendesk.com. This portal also allows end users to login to review the status of their tickets, and find additional information related to their support needs. The COHMIS Help Desk Portal is combined across all four HMIS Lead Agencies. If the information is unable to be resolved using the COHMIS Help Desk Portal, end users should contact their CoC's HMIS Lead Agency Helpdesk. For end users working in multiple CoC's, the ticket should be submitted to the HMIS Lead Agency with the most proximity to the client, project or issue.

CoC HMIS Lead Agency Helpdesks:

MDHI

Email: hmishelp@mdhi.org
Phone: 720-500-4116
Hours: Monday-Friday, 9-3

Balance of State

Email: colorado.hmis@coloradocoalition.org
Phone: 303-312-9666
Hours: Monday - Friday, 9-4

Pikes Peak

Email: hmishelpdesk@ppchp.org
Phone: 719-632-5094
Hours: Monday-Friday, 8-5

Northern Colorado

Email: hmis@homewardalliance.org
Phone: 970-430-6442
Hours: Monday - Friday, 9-3

8.3 Helpdesk Access Procedures

Agencies can initiate a request for assistance through the COHMIS Help Desk Portal, email or telephone, preferably in that order. It is important that all calls and emails to the Helpdesk are

processed in an efficient and effective manner. Emails and telephone calls will be responded to within 2 business days. To ensure that this goal can be achieved the following procedures should be followed:

Procedures:

1. While the Helpdesk strives to answer as many calls as possible during regular business hours, if a caller must leave a voicemail message, the message should include: the names of the caller, agency, and program; a return phone number; and the issue prompting the call. A staff member will respond within 2 business days to gather any further information needed to determine the appropriate resolution.
2. When contacting the Helpdesk, it is better to use email rather than telephone. Sending an email will allow you to include a screenshot of the error; screenshots go a long way in facilitating a quick problem resolution.
3. When contacting the Helpdesk via email, always refer to a client by their Unique Identifier. Do **not** transmit PII unencrypted.

9. HMIS Software Security

9.1 What is Security?

Security is the degree of resistance to, or protection from, harm or unauthorized access to electronic data. The security of the data held in our HMIS database is a high priority in our community. We take the confidentiality, integrity, and availability of all HMIS information seriously and understand that as stewards of client level data we must protect against any reasonably foreseeable threats or hazards to security and ensure that end users are in compliance with the standards set forth in this manual. Security breaches can be defined as network security breaches and data breaches.

9.2 Network Security Breach

While it may be impossible to totally avoid network security breaches, you can lessen the chance of a network intrusion by monitoring and changing employee passwords, backing up your network, and using experienced IT personnel to aid you in protecting the information your network contains.

9.3 Network Security System Level Prevention Measures

9.3.1 Server Level Security

Bitfocus owns and maintains its own physical servers and network infrastructure in a secure, US-based data center. Hosting facilities provide state-of-the-art security that enforces 24/7 physical and electronic security, including on-site security guards, trap-door entry, key card, and biometric access, and electronic surveillance and alarms. The Clarity HMIS software is secured

physically through several best practices, resulting in highly effective security at the most basic level. Several of these system-level security features include:

- Separation of the database and application on different servers
- Hardware Firewall that forwards only port 443 (Encrypted SSL) to the internal web server. A software firewall also protects each customer web server on the internal network. Multiple layers of firewalls between database, application, and users
- Encryption of the data on the database. All traffic is 2,048 bit SSL encrypted. All API traffic must be further encrypted.
- Access to the internal network is only possible via an encrypted VPN connection. Access to the internal network is only provided to Clarity Human Services staff and authorized system administrators.
- Undisclosed location of the physical servers
- Physical servers are locked down in secured, fire-safe rooms. Databases are housed on an internal server, inaccessible from the public network. This ensures that client data is protected by our multi-layer security systems and strict access policies.

9.3.2 Application Level Security

There are additional layers of security built into the Clarity HMIS software itself. This makes the system harder to access without appropriate permissions. These security features include:

- 128-bit encryption of the connection between an HMIS user's computer and the HMIS application
- Users are organized into security groups that are given specific permissions for what their members can access in HMIS
- Two-factor authentication
- A user's connection to the application automatically closes after a period of inactivity
- Logging and audit systems in the background automatically record each user's activities in adding, viewing, and editing information

9.4 Data Security Breaches

A data breach occurs when the steward (i.e., HMIS end user or agency staff) of information allows it to fall into the hands of an unauthorized party. This can involve data in any form including that which is printed or transmitted verbally, although in the digital age the term has generally come to refer to the transfer of electronically stored data. Partner Agency Agreements indicate that the Partner Agency can be held liable for any data breaches as a result of their staff's actions, and the HMIS Lead Agency is not liable for breaches or loss occurring as a result of HMIS end user or Partner Agency actions. Regardless, the HMIS Lead

Agency must be made aware of the breach per the protocol listed in the COHMIS Security, Privacy and Data Quality Manual.

9.4.1 Examples of Qualifying Data

- First name or first initial and last name
- Social Security number
- Driver's license or State Identification number
- Account number or credit card number
- Medical information
- Health insurance identification number
- Username or email address, in combination with a password or security questions and answers that may promote access to the account[9]

9.5 Data Security Breach Prevention Measures

9.5.1 Workstation Security Procedures

Statistically, most security breaches are due to human error rather than systematic issues. To keep the application and data secure, HMIS users must implement some additional security measures.

Procedure:

1. Do not write down your username and password. However, if that is not practical and you must write them down, do not store them in an unsecured manner (i.e., under the keyboard or on the monitor). Such practices can lead to security breaches. Instead, store them in a locked drawer or cabinet. We are the stewards of our clients' data.
2. Never share your login information with anybody (including site or system administrators). If someone is having trouble accessing HMIS, contact the Agency DPAL or the COHMIS Helpdesk. Sharing usernames and passwords is a severe violation of the HMIS End User Agreement. If you share your username and password with someone, anything they do in the system will be tracked to your user account. When administrators review the data and security logs, you will be held responsible for any HMIS activity that occurred under your login.
3. When you are away from your computer, log out of HMIS or lock down your workstation. Stepping away from your computer while you are logged into HMIS can lead to a serious security breach. Although there are timeouts in place to catch inactivity built into the software, they do not take effect immediately. Therefore, any time you

[9] https://www.dataprivacymonitor.com/data-breach-notification-laws/colorado-enacts-sweeping-changes-to-data-breach-reporting-requirements-and-adds-new-data-security-requirements/

leave your workspace and are no longer in control of the computer, you should lock down your workstation.

4. Your computer screen should be positioned so that it is difficult for others in the room to see the contents of the screen. The placement of monitors can play a major role in establishing security at the agency. Good placement: When someone walks into the room all they can see is the back of the monitor. Bad placement: When someone walks into the room, they can look over your shoulder without you knowing it and read material on the monitor.

9.5.2 Handling Client Level Data

To secure client level data, it is necessary to eliminate any opportunities for its unauthorized disclosure. Each HMIS user must take the necessary precautions when accessing and using clients' personally identifiable information. Whether it is in electronic or printed form, such information should never be displayed in public areas, faxed, kept on desks in unlocked offices, or distributed electronically. The CoC, and the agency's HMIS DPAL and Executive Director must be contacted within 24 hours if a data security breach is detected.

The COHMIS recommends these best practices:

- Limit access to all forms of personally identifiable information (name, birth date and SSN). Whenever possible strip names, birth dates and SSNs from reports. Provide this information only to people that "need to know" within the organization.
- Secure electronic files containing personally identifiable information on a network drive with limited access, and password protect such files (don't backup).
- Properly dispose of paper copies generated from HMIS by shredding them or storing them in a locked cabinet.
- Do not store or save files containing exported information (e.g., data exported to Excel or Access) on the following portable media.
- Client documents that are transported between locations or created in the field **must** be secured in a way that protects the client's information (e.g., a locked briefcase, or any other apparatus with a locking mechanism).

9.6 Security Auditing

DPALs or designated agency staff are required to resolve any issues uncovered during an HMIS Partner Agency monitoring. To maintain the highest level of security and protect client privacy and confidentiality as set forth in this manual, HMIS Lead Agencies will audit each Partner Agency's HMIS security compliance on an annual basis. DPALs will work with HMIS Lead Agencies to schedule and assist in the monitoring process. The monitoring will cover many topics (e.g., informed consent procedures, privacy and security practices, data entry practices) that are made available in the COHMIS Partner Agency Monitoring Protocol. More information about these audits can be found in the COHMIS Security, Privacy and Data Quality Manual. Any

identified deficiencies need to be resolved within the guidelines of the COHMIS Security, Privacy and Data Quality Manual.

10. HMIS Data and Reporting

10.1 HMIS Reporting Capabilities

Reporting is an important functionality of all databases. It is important that participating agencies see the benefits of entering data into HMIS and have the ability to use the information entered. HMIS has a robust suite of reports available to users, including application reports, management reports and ad-hoc reports.

10.2 Ownership of Client Level Data

The CoC and HMIS Lead Agency are the custodians of the client-level data that it has entered in HMIS, while the client is the owner of the data. Consequently, neither the CoC nor the HMIS Lead Agency will at any time change, distribute or delete such data without the permission of the agency overseeing that data. If an agency withdraws from participation in HMIS, its data will be kept for a minimum of seven years after withdrawal and may be included in CoC reporting or analyses. The HMIS Lead Agency reserves the right to use HMIS aggregate level data (i.e., data that is aggregated across all agencies participating in HMIS and that cannot be traced to individual clients) for the purposes of CoC management, reporting, decision making and analysis.

10.3 Access to CoC-Wide Data

CoC-wide data can play an important role in advancing the community's understanding of its homeless and at-risk populations. This information can help in planning future service offerings, identifying gaps in community services, analyzing the effectiveness of programs, and developing local and statewide policies that reduce the length of homeless episodes, decrease returns to homelessness, and ultimately end homelessness. To realize these benefits, the HMIS Lead agency may share HMIS aggregate level data with agency collaborations, state and local officials and researchers. All requests for aggregate level data must be initiated with the HMIS Lead Agency.

10.4 Distribution of HMIS Data

Requests for data aggregated across all clients served by a particular program or agency should be approved by the cognizant agency. The agency should be given the opportunity to process the request, and if they need assistance should contact the COHMIS Helpdesk.

Requests for data aggregated across the entire CoC should be sent to the CoC's HMIS Lead Agency. Once vetted, the HMIS Lead Agency will forward to the CoC for approval. If approved,

the request is processed by the HMIS Lead Agency, which will include a fee and time estimate if appropriate.

Requests for data aggregated statewide should be submitted to the CoC HMIS Lead Agency, who will work with the other CoC HMIS Lead Agencies to vet and will forward to the Collaborative for approval.

Requests for data aggregated across a collaborating group of participating agencies should be sent to the Collaborative Lead or its designee for approval. The Collaborative Lead should have in place a written agreement signed by each agency participating in the collaborative that grants the Lead access to the signers' data.

10.5 Funder Access

Entities providing funding to agencies or programs that are required to participate in HMIS will not have automatic access to HMIS. The funder should request HMIS aggregate, de-identified data from its grantee. The grantee will produce the report or submit a request to the HMIS Lead Agency, if needed. If the funder requires data aggregated across multiple grantee agencies, its contract with each grantee must state that the funder has the agency's permission to acquire such data. These aggregate requests should be submitted to CoC, which will require proof of the contracts between the grantees and the funder. Time and fees will be determined by the HMIS Lead.

10.6 CoC Access

The HMIS Lead Agency will provide monthly Data Quality Reports, Participation Reports and any reports necessary to support CoC funding processes. CoC-wide data will be provided to HUD annually as required for the AHAR/LSA reports, system performance measures and CoC grant applications.

The CoC reserves the right to publish a participating agency's aggregate data for the purposes of data quality improvement, compliance, analysis or decision making.

The four COHMIS Lead Agencies may also combine their aggregate data into a statewide report or dashboard for a view of homelessness across Colorado as a whole.

10.7 Researcher Access

COHMIS recommends that prior to obtaining HMIS data, academic researchers must execute written research agreements with the CoC or the participating agencies from which data are sought. Personally identifiable information will not be released, unless such disclosures are detailed in the approved research agreements. COHMIS also requires that written research agreements address the rules for data use, the limitations of the data, how the data will be stored, and data security and disposal procedures. Data requests that do not require personally identifiable information may not require a research agreement. Requests for statewide data will be considered by the Colorado Statewide HMIS Collaborative, which meets monthly.

Requests for CoC data will be made by each CoC Lead. Time and fees will be determined by the HMIS Lead.

10.7.1 Anonymization of Data

Only Anonymized Data will be released to researchers. The provider shall remove all personal identifiers which can be used to distinguish or trace an individual's identity. Personal identifiers shall include those consistent with a HIPAA Limited Data Set, which include full name, date of birth, social security number and all contact information (including phone number and residential address smaller than town or city).

10.7.2 Cell Suppression Policy

The Cell Suppression is the amount of observations needed to display the desired data results. The Policy stipulates that no cell (e.g., grouping of individuals, patients, clients) may be displayed without the number of observations predetermined by the provider. Also, no use of percentages or other mathematical formulas may be used if they result in a cell displaying less than the predetermined amount of observations. Individual level records may not be published in any form, electronic or printed.

10.8 Release of HMIS Data by Participating Agency

All participating agencies are responsible for ensuring the confidentiality of the information held in Colorado's HMIS database. Each agency is responsible for ensuring that all data within HMIS is held to the strictest confidentiality standard possible.

Release of Information Policy:

> Partner Agencies may disclose information that was not obtained from HMIS (i.e., information that an agency develops through its own administrative or research efforts, without accessing HMIS) as they see fit. However, except as specified in the next paragraph, Partner Agencies should never release data or information obtained from HMIS to any party without the permission of their HMIS Lead Agency. If required by any court of competent jurisdiction in the state of Colorado. Court orders should be directed to the CoC.

At no time should hard copies or electronic copies of HMIS forms be released without the permission of the HMIS Lead Agency. If a Partner Agency receives a request for HMIS information, the requestor must be directed to contact the HMIS Lead Agency. Should a Partner Agency find that there has been an unauthorized release of data obtained from HMIS, it must contact the HMIS Lead Agency immediately and no later than one business day after the date of discovery. Failure to do so will be considered a breach of this policy.

Agencies may share information obtained from COHMIS under the following circumstances:

- In an immediate life-threatening situation that involves a staff member or a client in the agency's care
- If a staff member or volunteer suspects abuse or neglect of a child or elderly person

In the above situations, Partner Agencies should follow internal protocols and send an incident

report to the HMIS Lead Agency within one business day.

Procedure in the Event of a Breach:

- Should it be determined that an agency released information without receiving permission from COHMIS, an investigation will be conducted by a committee comprising members of the CoC where the breach occurred (one member of the CoC's Lead Agency staff, one member of the CoC's HMIS Lead Agency staff, and one member of the CoC's Board of Directors) and a representative of the Statewide Collaborative from one of the other three Colorado CoCs. The findings of the investigative committee will be presented to the CoC Board of Directors and to the Statewide Collaborative. Each CoC Board of Directors will be responsible for determining consequences in the event of a breach. If it is found that a policy breach did occur, the consequences may range, without limitation, from revocation of database privileges up to and including the suspension of the agency's HUD NOFA funding.

11. Coordinated Entry

11.1 Definition of Coordinated Entry

Coordinated entry is a process developed to ensure that all people experiencing a housing crisis have fair and equal access and are quickly identified, assessed for, referred, and connected to housing and assistance based on their strengths and needs. This document answers several frequently asked questions about coordinated entry and HMIS.[10]

11.1.1 Background

HUD requires each CoC to establish and operate a "centralized or coordinated assessment system" (referred to as "coordinated entry" or "coordinated entry process") with the goal of increasing the efficiency of local crisis response systems and improving fairness and ease of access to resources, including mainstream resources. Both the CoC and ESG Program interim rules require use of the CoC's coordinated entry process, provided that it meets HUD requirements. Coordinated entry processes are intended to help communities prioritize people who are most in need of assistance. They also provide information to CoCs and other stakeholders about service needs and gaps to help communities strategically allocate their current resources and identify the need for additional resources. The CoC Program interim rule set the basic parameters for coordinated entry and left further requirements to be set by HUD notice. Since the CoC Program interim rule was published in 2012, HUD has learned a great deal about what makes a coordinated entry process most effective and has determined that additional requirements are necessary. Updated guidance is available from HUD on best practices on data management.[11] This Notice establishes those additional requirements.[12]

11.1.2 Coordinated Entry in Colorado

Coordinated entry operates differently across the four CoCs in Colorado. Each CoC has a specific coordinated entry policy and procedure manual to be used in conjunction with the COHMIS Statewide Policies & Procedures.

- In Metro Denver, the coordinated entry system is called OneHome and more information is available at www.onehomeco.org
- In El Paso County, the coordinated entry (CE) system information is available at https://www.ppchp.org/programs/continuum-of-care/coordinated-entry-ce/
- In Balance of State, the coordinated entry system is governed by CoC-wide P&P's and tailored to each regional coalition. More information is available at https://www.coloradocoalition.org/BoSCoCCES
- In Northern Colorado, the coordinated entry system is called Coordinated Assessment and Housing Placement System (CAHPS) and more information is available at https://www.nocococ.org/cahps

[10] https://www.hudexchange.info/resources/documents/Coordinated-Entry-and-HMIS-FAQs.pdf

[11] https://www.hudexchange.info/resources/documents/coordinated-entry-management-and-data-guide.pdf

[12] Authority established in 24 CFR 578.7(a)(8), "This system must comply with any requirements established by HUD by Notice.