# Comprehensive HMIS Policies and Procedures Manual

Cincinnati/Hamilton County CoC, Strategies to End Homelessness HMIS Lead

# 1 Introduction

HMIS is a computer system that collects information about the experiences and needs of people experiencing homelessness or having trouble with housing. Strategies to End Homelessness (STEH) manages the HMIS. Clarity Human Services is the HMIS software. HMIS is required by law (The HEARTH Act, put into law on May 20, 2009) for communities that receive certain funding. The U.S. Department of Housing and Urban Development (HUD) and the federal partners define what data is collected, along with some data points decided by our community.

This manual is meant to guide and explain federal rules related to HMIS for Cincinnati/Hamilton County Continuum of Care (CoC) OH-500 agencies. This document is not a substitute for any federal rules.

## 1.1 HMIS Lead Agency Contact Information

| | |
|---|---|
| KManning@end-homelessness.org | Kim Manning, STEH HMIS Director |
| HMISsupport@end-homelessness.com | HMIS Support Email – contact STEH HMIS Administrators to ask questions, request help, or ask for new reports or features |
| 513 – 263 - 2790 | HMIS Support Phone Number open Monday – Friday 9:00am-3:00pm (except STEH holidays) |
| https://steh.freshdesk.com/support/solutions | HMIS Support Knowledgebase with step-by-step guides and information on most HMIS features and processes written and updated by the STEH HMIS Administrators |
| https://tinyurl.com/2p92tzey | Strategies to End Homelessness YouTube Channel with videos showing many HMIS processes. |
| https://steh.talentlms.com/ | HMIS Training Courses<br>On Demand Course List : (freshdesk.com) |
| https://help.bitfocus.com | Help articles published by the HMIS vendor Bitfocus |
| https://www.strategiestoendhomelessness.org/what-we-do/data/hmis-transition/ | HMIS Policy Documents |

## 1.2 Definitions

**Cincinnati/Hamilton Continuum of Care (CoC)** - a funding and planning method that helps communities plan and provide services for people and families experiencing homelessness or at risk of homelessness. HUD also refers to the group of organizations and people involved in the decision-making process as the "Continuum of Care."

**Homeless Clearinghouse** – The Cincinnati/Hamilton County CoC Board is known locally as the Homeless Clearinghouse. The CoC board is a group of people selected to provide oversight and authority for the CoC. The board includes representatives from organizations who serve people and families experiencing homelessness or housing trouble, other interested people or organizations dedicated to dealing with homelessness, and people who have experienced homelessness.

**CoC Lead/Unified Funding Agency (UFA)**– Strategies to End Homelessness (STEH) is selected by the CoC to be the Cincinnati/Hamilton County CoC Lead to carry out the duties in the CoC Program Interim Rule. STEH is also selected by the CoC to apply for Unified Funding Status to receive and distribute money available for projects in the CoC. The Homeless Clearinghouse and HUD must approve STEH's UFA status each year.

**Homeless Management Information System (HMIS) -** a computer system approved by the CoC and meets legal standards to collect information about the experiences and needs of people experiencing homelessness or having trouble with housing.

**HMIS Lead** - Strategies to End Homelessness (STEH) is selected by the CoC to assist users and manage the HMIS.

**HMIS Administrators** – People who setup and maintain the HMIS and research tools including members of STEH's HMIS Department who provide user support, training, and manage the HMIS; administrators employed by the HMIS vendor; and people employed to maintain data research tools.

**Covered HMIS Organization (CHO)** - an organization that provides services to people and families experiencing homelessness or housing trouble and enters data into HMIS. Or any other approved organization that accesses HMIS directly for other purposes such as system administration or research.

**CHO HMIS Primary Point Person (PPP) –** the first person STEH HMIS Administrators contact to approve users or answer questions. The CHO HMIS PPP will attend meetings to hear updates about HMIS and share HMIS information with the organization.

**CHO Security Officer** – a staff member selected by a CHO to complete a yearly security review and make sure the CHO is in line with HMIS security standards (this can be but does not have to be the same person as the CHO PPP).

**HMIS User(s)/User(s)** – a person who works for a CHO and enters data or works with data in HMIS.

**Project Participant/Participant**– a person or family who receives services from a CHO and whose data is entered into HMIS.

**Victim Services Provider (VSP)** – an organization whose main mission is to provide services to victims of domestic violence, dating violence, sexual attack, or stalking.

**Personally Identifiable Information (PII) or Protected Personal Information (PPI)** - any information that can be used to identify a person or family whose information is entered into HMIS.

**Program or project** – services offered by a CHO are grouped based on the grant paying for the services. HUD refers to these as projects, but they are referred to as programs in HMIS. Therefore, the terms project and program are used to mean the same thing for the purpose of HMIS.

For more key terms, definitions, and acronyms, HMIS, CoC, and other Acronyms : (freshdesk.com) or Homeless Management Information Systems - Implementation Guide - Glossary (hud.gov)

# 2 HMIS Governance Charter

## 2.1 Purpose

The CoC Governance Charter assigns Strategies to End Homelessness as the HMIS Lead Agency. The HMIS Governance Charter describes the roles and responsibilities related to the decision-making and operation of the Cincinnati/Hamilton County HMIS.

The United States Department of Housing and Urban Development (HUD), directed by the United States Congress, requires all organizations granted money for services to enter data into HMIS. Organizations that provide services to people and families experiencing homelessness or housing trouble who are not granted money may also enter data into HMIS to help the community work toward ending homelessness.

The HMIS and its policies and procedures follow the rules and guidelines released by HUD. The CoC may also require additional rules and guidelines needed for our community.

The HMIS Lead analyzes HMIS data to improve services and work to end homelessness. The HMIS Lead also uses aggregate data (that does not include PII) to report to federal, state, and local funders including:

- National reports such as the Longitudinal Data Analysis (LSA), System Performance Measures (SPM), the Housing Inventory Count (HIC) and Point in Time Count (PIT), the Annual Performance Report (APR), and the Consolidated Annual Performance and Evaluation Report (CAPER).
- Planning activities to reduce homelessness for Cincinnati and Hamilton County

The CoC Governance Charter, HMIS Governance Charter, and all HMIS policies and procedures are reviewed (or updated) and approved each year.

## 2.2 Key Roles and Responsibilities

The roles and responsibilities included below may not include everything needed. It is important for the CoC, CHOs, HMIS users, the HMIS Lead, the Homeless Clearinghouse, and everyone noted below to work together to solve problems and to have a successful HMIS.

### 2.2.1 The Homeless Clearinghouse (Continuum of Care Board)

i. Selects a single qualified organization to manage the CoC's HMIS each year, which will be known as the HMIS Lead.
ii. Selects a single Homeless Management Information System (HMIS) for the Cincinnati/Hamilton County (approved each year).
iii. Reviews, revises, and approves the HMIS Governance Charter and HMIS policy and procedure documents including:
    a. Comprehensive HMIS Policies and Procedures Manual
    b. HMIS Agency Participation Agreement
    c. HMIS User Agreement and Code of Ethics
    d. HMIS Client Consent Form and Privacy Notice
iv. Makes sures, at a minimum, organizations granted money from HUD or the UFA provide data to HMIS; and encourages all organizations which serve people and families experiencing homelessness to provide data to HMIS even if the organization is not granted money.
v. Makes sure the HMIS is managed in agreement with HUD rules and guidelines.

### 2.2.2 Strategies to End Homelessness (STEH), UFA and CoC Lead

i. Makes sure HMIS meets HUD's rules and regulations.
ii. Encourages and helps organizations providing services to address homelessness to participate in the HMIS.
iii. Makes public all relevant CoC and HMIS meetings, inviting participation from the HMIS community at large.
iv. Consult with the full CoC to develop HMIS policies and procedures in agreement with HUD rules and regulations.
v. In discussion with and subject to oversight of the Homeless Clearinghouse, negotiates, approves and executes contract(s) with the HMIS vendor.

### 2.2.3 Strategies to End Homelessness (STEH) HMIS Lead

i. Supervises the HMIS project and has the main responsibility for all HMIS activities.
ii. Makes decisions related to the day-to-day operations of the HMIS.
iii. Makes sure HMIS is in agreement with HUD rules and regulations and writes policies and procedures for the CoC.
iv. Monitors and enforces data quality based on the HMIS Policies and Procedures Manual and Data Quality Plan and to meet reporting expectations.
v. Participates in and represents the CoC to regional or national HMIS-related organizations.
vi. Supervises contract(s) with HMIS vendor(s).
vii. Provides initial and on-going training and support to HMIS users.
viii. Manages data sharing agreements between CHOs as needed.
ix. Works with the Homeless Clearinghouse to manage HMIS continuing quality improvement.
x. Assign at least one staff member as the HMIS Lead security officer.
xi. Run system-level and project-level reports for submission to local, state, and federal partners.
xii. Follow the most recent HMIS Policy and Procedures Manual (Policy) approved and adopted by the Homeless Clearinghouse. Including the HMIS Data Quality Plan, HMIS Data Privacy Plan, and HMIS Security Plan.
xiii. Make sure that all employees and agents also follow the established policies and procedures.
xiv. Participate in monitoring and oversight procedures as conducted by the CoC Lead on behalf of the Homeless Clearinghouse.
xv. Choose an HMIS Lead Security Officer to be responsible for making sure HMIS services are conducted in a secure manner and hold the HMIS vendor accountable for HMIS security as required by the Homeless Management Information Systems (HMIS); Data and Technical Standards Final Notice.
xvi. HMIS System Administration including but not limited to:
    a. User support and training including on-going annual training required to maintain access to HMIS.
    b. HMIS Help Desk and support ticketing system
    c. Communications with CHOs and HMIS Users
    d. User account management
    e. HMIS project and reporting customizations
    f. Confirm that HUD required reporting is functional and correct

### 2.2.4 Covered Homelessness Organizations (CHOs)

i. Play a leadership role in the success of the HMIS.
ii. Execute and comply with an HMIS Agency Partner Agreement and, if needed, an agency partnership data sharing agreement.
iii. Create HMIS policies and procedures that meet federal, state, and local rules and guidelines needed by the CHO.

iv. Follow the most recent HMIS Policy and Procedures Manual (Policy) approved and adopted by the Homeless Clearinghouse. Including the HMIS Data Quality Plan, HMIS Data Privacy Plan, and HMIS Security Plan.
v. Make sure that all employees and agents also follow the established policies and procedures.
vi. Participate in monitoring and oversight procedures as conducted by the HMIS Lead on behalf of the Homeless Clearinghouse.
vii. Choose a Primary Point Person(s) who will be the main point of contact for the HMIS Lead.
viii. Choose an HMIS Security Officer to be responsible for making sure the CHO meets the HMIS security guidelines (this can be the same person as the Primary Point Person or a different person).
ix. Notify the HMIS Lead/HMIS Administrators of new or terminating users.

### 2.2.5 CHO Primary Point Person

i. Attend HMIS meetings and/or communicate regularly with the HMIS Lead.
ii. Make sure the CHO meets the rules and guidelines written in the HMIS policies and procedure documents.
iii. Troubleshoot HMIS issues.
iv. Approve HMIS users.
v. Provide HMIS support for the CHO as needed.
vi. Advise and recommend changes to HMIS Policies and Procedures, data collection, and reporting on behalf of their CHO and users.

### 2.2.6 CHO and HMIS Lead HMIS Security Officers

i. Must be familiar with the HMIS Self-Monitoring Checklist to make sure the CHO meets HMIS security standards.
ii. Complete or supervise security tasks/process listed in the HMIS Self-Monitoring Checklist at least yearly and keep a written record of the results.

### 2.2.7 HMIS Users

i. Sign an HMIS User Agreement yearly.
ii. Strictly follow the commitments made in the HMIS User Agreement and Code of Ethics.
iii. Make sure HMIS data is kept private as expected by the individuals and families they work with.
iv. Report any security violations to the CHO PPP and/or HMIS Lead.
v. Follow all policies and procedures described in HMIS policy and procedure documents and HMIS training courses.
vi. Not share their HMIS username or password under any condition and be held responsible for actions taken under their username and password.
vii. Participate in HMIS training including yearly HMIS security training.
viii. Enter truthful data based on what the individual or family reports to them or based on the actions taken by the user or CHO for the person or family.

### 2.2.8 Victim Services Provider (VSP)

Victim Service Providers are required to *not* participate in the community's HMIS. They must collect HMIS required data in a "Comparable Database." The Comparable Database must meet the requirements and guidelines listed in the HMIS Comparable Database Manual provided by HUD, provided by the Violence Against Women Act (VAWA), and required by Homeless Management Information Systems (HMIS); Data and Technical Standards Final Notice.

# 3 HMIS Policies and Procedures

## 3.1 HMIS Users

### 3.1.1 User Access

**Policy**: HMIS Users must:

- Complete required HMIS training courses.
- Understand and commit to follow the HMIS User Agreement and Code of Ethics and the HMIS Client Consent Form and Privacy Notice.
- Only enter or access HMIS data related to their job responsibilities.
- Follow the HMIS policies and procedures noted in this document.
- Keep their HMIS username and password private and never share them with anyone for any reason.

**Procedure**:

1. Each HMIS User must read and sign the HMIS User Agreement and Code of Ethics which includes the HMIS Client Consent Form and Privacy Notice before using the HMIS and each year they use HMIS. By signing the user promises:
    a. Never share their username or password with anyone for any reason.
    b. Only enter or access HMIS records needed for their job responsibilities.
    c. Follow the rules and guidelines noted in this document.
2. HMIS Users will not be given access to HMIS unless all required training courses and agreements are completed as needed.
3. Users with access to HMIS must maintain required annual HMIS training. Failing to complete required annual training will result in the user's access to HMIS being stopped until the required training(s) have been completed.

### 3.1.2 Program Participant Authority to Keep Data Private

**Policy**: Program participants have the right to request their HMIS record or specific HMIS entries be kept private. HMIS users have the responsibility to set the participant's record or specific entries to private so the record or entry(ies) are not shared broadly in the HMIS.

**Procedure**:

1. HMIS users must complete the required HMIS training and know how to set participant records or specific entries to private.
2. Users will review and explain the HMIS Client Consent Form and Privacy Notice with each person/family they work with at least every 7 years.
    a. Users will make sure participants are aware they can request specific data entries (enrollments, assessments, services/service notes, client notes, referrals, files, and exits) be set to private and not shared broadly with other agencies.
    b. The head of household of a family may decide permission to share data for dependent children.
    c. The HMIS Client Consent Form and Privacy Notice should be reviewed with each adult in a household if possible. However, the families head of household may decide permission to share data for other adult household members if the other adults in the household are not available.

d. Documenting the ROI in Clarity confirms the HMIS Client Consent Form and Privacy Notice was reviewed with program participant. Documenting permission as "No" confirms HMIS Client Consent Form and Privacy Notice the was reviewed with the participant and they chose not to share information with other agencies in HMIS. Documentation may be imported from other systems if the agency enters data directly into an alternative system and imports data into HMIS.

3. Users will document each person/family's permission or non-permission to share information in HMIS.
4. Users will set requested data to private.
5. Users may contact HMIS for assistance or additional training.
6. Services may never be denied because a participant refuses to share data in HMIS or because a participant refused to provide their information. *(ref: 2024 Data Standards Manual pg. 50)*

### 3.1.3 Mentions of Caracole or YWCA Set to Private

**Policy**: Any data referencing the YWCA or Caracole will be kept private based on providing services to special populations.

**Procedure**:

1. Users will complete the required training to understand and know how to set any data referencing the YWCA or Caracole to private.
    a. YWCA users will not enter data directly into the community's HMIS.
    b. HMIS Administrators will import Caracole data into a secure agency in Clarity which is not shared with other CHOs.
    c. Caracole HMIS Users will only enter or edit Caracole specific data into the secure agency in Clarity which is not shared with other CHO's but will be able to set a record to shared if specifically requested by the participant.
2. HMIS users will set any reference to the YWCA or Caracole to private, including services/service notes, client notes, referrals, files, or any other type of data entry.
3. Users may contact HMIS for assistance or additional training.

### 3.1.4 Ethical Data Entry

**Policy:** HMIS Users will:

- Enter data provided by program participants based on what the program participant says.
- Enter or upload data about services and support provided by the CHO as correctly and truthfully as possible.
- Enter all notes and comments in a respectful professional manner.
- Never enter or upload data that includes offensive or discriminatory comments about a program participant.
- Never upload material that violates any federal, state, or local laws (copyrighted, threatening or obscene, or known to include trade secrets.)

**Procedure:**

1. HMIS Users will participate in Ethical Data Entry training to access and maintain access to HMIS.
2. Failure to complete the training will result in HMIS access being ended.
3. If unsure, HMIS Users will ask their supervisor or CHO PPP for assistance determining if their data entry or file uploads meet the guidelines for ethical data entry.

## 3.2 Imported Data Policy for CHOs and Users

Some CHOs choose to directly enter data into a different system and import data into HMIS. All users and CHOs working with HMIS data must follow the policies and procedures that apply to their work whether they have direct access to HMIS or not.

All data entered in other systems are not imported into HMIS. It is important CHO PPPs, HMIS users, and users who enter data into the other system know what data is imported into HMIS, and when data must be set to private in HMIS.

Data imported from VESTA is imported twice each day through an automated process known as an API. Data imported from other sources (ETO, HOMES, etc.) are imported manually by HMIS Administrators. Procedures for working with imported HMIS data require different approaches. This is because the way data is imported is different from how it is entered manually.

### 3.2.1 Setting Imported Data to Private

**Policy:** CHOs who import data into HMIS must make sure data is set to private in HMIS if the participant requests their data is not shared with other CHOs or if imported data includes references to the YWCA or Caracole.

**Procedure for Setting Entire Record to Private from VESTA:**

1. Participant records imported from VESTA into Clarity cannot be set to private. Any participant who does not sign the HMIS Privacy Notice and Client Consent Form must be entered directly into HMIS, set to private in Clarity, and ***not* entered in VESTA**.
2. If the participant has previously signed a HMIS Privacy Notice and Client Consent Form, they have agreed to share their basic information (on the Profile screen in Clarity). That data is already shared and cannot be unshared. In this case, users may enter the participant's data into VESTA and then follow the "Procedure for setting Enrollment or specific data element to private in VESTA" below.

**Procedure for Setting Enrollment or Specific Data Elements to Private from VESTA:**

1. The data must be imported into Clarity before it can be set to Private. Check Clarity for the participant's record after the next import and again the following day if the record is not found.
    a. Contact HMISsupport@end-homelessness.org if the participant's record does not show up in Clarity within two days.
2. Follow the instructions for setting the enrollment or other data to private (provided through HMIS training, HMIS support articles, or request assistance from HMISsupport@end-homelessness.org). Please keep in mind HMIS Administrators may not be aware if the participant has requested their enrollment or other data be set to private. Therefore, it is important that CHOs and Users take needed action(s) on the participant's behalf.

**Procedure for Setting Data to Private or Shared from ETO (Caracole)**

1. All Caracole data imported by HMIS Administrators will be set to Private.
2. Caracole participants who request their data be shared with other CHOs in HMIS should be documented by signing a HMIS Privacy Notice and Client Consent Form.
3. Caracole staff may follow instructions for sharing records (provided through HMIS training, HMIS support articles, or request assistance from HMISsupport@end-homelessness.org) for participants who request their Caracole data is shared with other CHOs.

4. Caracole participant records should not be shared in HMIS unless the participant has a signed HMIS Privacy Notice and Client Consent Form documented in Clarity.

**Procedure for Setting Data to Private for Other CHOs Whose Data is Imported Manually by HMIS Administrators**

1. The CHO provides a data set to be imported into HMIS.
2. The CHO must also tell HMIS Administrators of any participant whose record should be imported set to private *before* the data is imported into HMIS.
    a. If the CHO is unable to notify HMIS Administrators in advance, the CHO should enter the participant's data directly into HMIS, set the record to private, and not enter the data in the other data system.
3. If requested by participant(s), the CHO will set enrollments or other data points to private after the data has been imported into HMIS.
    a. The CHO will confirm with HMIS Administrators when the data will be imported into HMIS.
    b. The CHO will follow the instructions for setting the enrollment or other data to private (provided through HMIS training, HMIS support articles, or request assistance from HMISsupport@end-homelessness.org) within two business days of the data being imported.
    c. Please keep in mind HMIS Administrators may not be aware if the participant has requested their enrollment or other data be set to private. Therefore, it is important that CHOs and Users take needed action(s) on the participant's behalf.

## 3.3 Covered Homeless Organization (CHO)

### 3.3.1 HMIS Policy Development

**Policy:** All OH-500 CHOs are responsible for maintaining their own HMIS policies and procedures that:

- Agree with federal, state, and local regulations and any related outside regulations.
- At a minimum, include the policies and procedures within this document unless covered under HIPPA.
    - CHOs covered under HIPAA are not required to comply with the HMIS privacy or security standards to avoid conflicts between the two sets of rules. Their policies and procedures would reflect HIPAA privacy and security standards.
- CHOs may include additional rules and guidelines, beyond the community HMIS or HIPAA rules and guidelines. These must be reflected in the CHO's specific policies and procedures.

**Procedure:**

1. CHOs will provide their HMIS Policy and Procedures documentation upon request.
2. CHOs will show that their HMIS Policies and Procedures are at least aligned with or refer to this document or HIPAA as appropriate.
3. CHOs will demonstrate their HMIS Policies and Procedures are made available to all staff who use HMIS or use data for or from HMIS by either:
    a. Demonstrating the CHO's HMIS Policies and Procedures are included with new hire packets or staff training processes.
    b. Demonstrating HMIS Policies and Procedures are available on the CHOs internal or external website.

### 3.3.2 User Access

**Policy**: Each CHO must make sure that only approved users access HMIS. Only actively engaged staff, in their status as paid employees, contractors, volunteers, or associates may be users.

**New User Procedure:**

1. Submit a new user request form or email HMISsupport@end-homeless.org.

2. HMIS administrators will ask the CHO PPP to approve the request unless the request comes from the CHO PPP.
3. The CHO PPP will be notified when the user has completed the required training and is set up in HMIS or if there are any concerns about the request. (Users will need to sign an HMIS User Agreement and Code of Ethics before they are able to access data in the HMIS).

**User Termination Procedure:**

1. The CHO PPP will email HMISsupport@end-homelessness.org. Requests must be made before or within one business day (Monday – Friday) after the user's access should be ended.

### 3.3.3 Participant Requests for Data, Questions and Grievance

**Policy**: CHOs will maintain a written procedure for responding to requests to view or correct, questions about, and complaints related to HMIS data or data collection. The procedure must include, at a minimum, how requests, questions, and complaints may be submitted (e.g., orally, in writing, if there's a specific form), to whom they should be submitted, who is involved in considering and responding to the request, and how a response will be communicated to the participant. The procedure should include a timeline for when responses can be expected. *(ref: https://www.federalregister.gov/d/04-17097/p-591)*

**Procedure**:

1. CHOs will develop and maintain a written procedure for handling requests for, questions about, and complaints related to HMIS data, data collection, or security.
2. Written procedures will be made available to all participants by one or more of the following:
    a. Procedures will be posted on the CHO's website.
    b. Procedures will be posted in intake areas or other areas frequented by program participants.
    c. Procedures will be provided with program intake packets.
3. CHOs will send participant complaints and documented resolution to HMISsupport@end-homelessness.org.
4. CHOs will request the HMIS Lead assists with resolving requests, questions, or complaints about HMIS data or HMIS processes as needed.

### 3.3.4 On-going User Monitoring

**Policy:** CHOs will monitor their staff who use HMIS or access data for or from HMIS to make sure users and staff follow the policies and procedures noted in this document, the HMIS User Agreement and Code of Ethics, and the HMIS Privacy Notice and Client Consent Form.

**Procedure for ongoing monitoring:**

1. CHOs will use staff supervision, existing reports, participant record reviews, or custom requested reports to make sure the CHO's HMIS data entry is correct, follows the ethical data entry, and all HMIS policies and procedures.
    a. CHOs will use the [HUDX-225] HMIS Data Quality Report [FY 2024] report to monitor data collection at least monthly and take corrective action as needed. In addition to monitoring data quality issues CHOs should confirm the Report Validation Table for accuracy.
    b. CHOs will review the one of the available data quality dashboards or request customizations to monitor that participants agreement with the HMIS Privacy Notice and Client Consent Form is consistent with the participants sharing settings.

c. CHOs may opt to use reports available from the Data Analysis tab to further monitor services documented in HMIS, entry – exit dates and length of stay, project outcomes, participant demographics, and project set-up/users accessing the system.
d. CHOs will use case conferencing (including reviewing notes and services), staff supervision, and participant interviews to make sure users are following HMIS policies.
e. CHOs may opt to request custom reports be developed to assist with additional monitoring. These reports may be made available to all system users if HMIS Administrators determine they will provide value beyond the CHO who requested the report.

**Procedure for addressing monitoring concerns:**

1. CHOs will take steps to address monitoring concerns which may include additional training, additional supervision, or other strategies to increase accountability and correction.
2. CHOs may request additional support and individual or group training from HMIS Administrators.
3. HMIS Administrators will notify HMIS CHO PPPs and the user(s) of any concerns that may present through user support and training activities.
4. CHOs and HMIS Administrators will follow the security breach process documented in the HMIS Security Plan for any issues that represent a security breach.

### 3.3.5 User Grievance

**Policy**: CHO's will take the lead on HMIS User grievances to make sure the CHO is aware of the user's issue(s) and the HMIS Lead's response(s).

**Procedure:**

1. Users will report HMIS grievances to the CHO PPP.
2. The CHO PPP will report all HMIS-related user grievances to STEH HMIS Administrators at HMISsupport@end-homeless.org or the HMIS Director.
3. STEH HMIS Administrators or the STEH HMIS Director will provide an initial response to the grievance within 10 days.
4. HMIS Administrators will work with the User and CHO to identify a plan for a resolution. The plan will include a timeline and action steps.
5. The CHO PPP will be included on all communications about the grievance, face-to-face or phone/virtual conversations will be summarized and sent to the CHO PPP and user.
6. The CHO PPP may contact STEH Leadership if the user is not satisfied with the resolution provided by STEH HMIS Administrators.

### 3.3.6 HMIS Monitoring

**Policy:** CHOs will monitor their data quality, privacy, and security as required by HMIS Data Quality, Security and Pricay Plans included in this document. And will provide information and documentation needed for the yearly HMIS monitoring visit.

**Procedure for internal, on-going HMIS monitoring:**

1. Monitor data quality at least monthly
    a. Download and save a timestamped PDF file of the HUD HMIS Data Quality Report at least monthly for each HMIS project.
    b. Notify staff of data corrections needed.

c. CHOs may opt to download a new version of the HUD HMIS Data Quality Report which reflects the corrected data.
d. CHOs will develop a data quality improvement plan for individual staff or projects to address persistent data quality issues as needed.
e. CHOs and HMIS users may contact STEH HMIS Adminstrators with any questions or assistance resolving issues.

2. Complete a 'Self-monitoring privacy & security checklist' each year.
3. Make sure there is at least one active HMIS CHO PPP and HMIS Security Officer at all times.
4. Get at least one background check on the person assigned as the HMIS Security Officer within the time they are employed by the CHO (a background check at the time of employment is fine).
5. Make sure the CHO policies and procedures to manage HMIS data requests, questions, and grievances is updated and available.
6. Make sure the HMIS Privacy Notice and Client Consent Form is posted in intake areas and available on the CHO's website.
7. Make sure the CHO's procedures to limit internal access to data is updated and available.
8. Make sure the procedure of what to do in event a security or privacy violation occurs is updated and available.
9. Use the CHO HMIS Overview report often to make sure the list of HMIS users is accurate.
10. Keep updated notes of how and where each user accesses HMIS.
11. Make sure the CHO has a current, signed Agency Participation Agreement.

**Procedure to prepare for yearly HMIS monitoring visit**:

1. The following documentation will be required in advance of the monitoring visit:
    a. Monthly time stamped HUD HMIS Data Quality Reports
    b. CHO specific HMIS privacy and security policies and procedures if different from the community HMIS privacy and security policies and procedures listed in this document.
    c. Self-monitoring privacy & security checklist, completed by agency in past year.
    d. Provide the names of the active HMIS CHO PPP(s) and HMIS Security Officer.
    e. Background check for the HMIS Security Officer if not previously provided.
    f. CHO's procedure to address HMIS questions or complaints from participants and HMIS users.
    g. Policy limiting internal access to data.
    h. Internal procedure to be used in the event of a security or privacy violation.
    i. URL link to where the Privacy Notice & Client Consent Form is posted on your public-facing website (if available).
    j. List of all persons with an account in Clarity. Please note if they use Clarity on a computer, mobile device, or both. Also note each user's main working location (e.g. WFH, agency's main office, etc.).

## 3.4 STEH HMIS Administrators

### 3.4.1 User Access

**Policy**: Approved users who complete and maintain the needed training and agreements; and follow the HMIS rules and guidelines will have access to HMIS.

**New User Procedure**:

1. The CHO PPP or CHO Executive Director will be asked to approve all HMIS users before they are given access to HMIS.

2. New users will be given access to HMIS training and must complete the training and the hands-on activities before being provided access to the HMIS.
3. New users will be given a username and temporary password to HMIS after approval is received and training has been completed.
4. The new user must complete the following steps in the HMIS system before they are given access to HMIS data:
    a. Read and sign the HMIS user Agreement and Code of Ethics.
    b. Create a new, private HMIS password.
    c. Set up two factor authentication as an added layer of privacy and security
5. The user will be provided access to information and processes that directly relate to their job responsibilities based on the information provided by the CHO.

**On-going User Management Procedure:**

1. Users must read and sign a new HMIS User Agreement each year to continue accessing HMIS.
2. Users who have not accessed HMIS within 90 days will be set to inactive. Users may request these accounts be reactivated. HMIS Administrators may require approval from the CHO or updated training prior to reactivating the user's account if the user has not accessed the system in several months or if there are other concerns.
3. Users must complete all required on-going training to maintain access to the HMIS.

**User Termination Procedure**:

1. HMIS Administrators will terminate access to HMIS upon request by the CHO and will send an email confirmation when access has been terminated.
2. HMIS Administrators must terminate access to HMIS for any user who fails to follow the HMIS User Agreement and Code of Ethics or the HMIS security policies and procedures included in this document. The user and the CHO PPP will be notified by email if this situation occurs.

### 3.4.2 Mentions of Caracole or YWCA Set to Private

**Policy**: Any data entered by or referencing the YWCA or Caracole will be kept private based on providing services to special populations.

**Procedure**:

1. HMIS Administrators will provide training so users understand how to set any data entered by or referencing the YWCA or Caracole to private.
    a. YWCA users will be trained not to enter data directly into the community's HMIS.
    b. HMIS Administrators will import Caracole data into a secure agency in Clarity which is not shared with other CHOs.
    c. Caracole HMIS Users will be trained to only enter or edit Caracole specific data into a secure agency in Clarity which is not shared with other CHO's.
2. HMIS Administrators will monitor data entries (notes, services/service notes, referrals/referral notes, CE events/event notes) for references to Caracole or the YWCA.
3. Any references to the YWCA or Caracole not set to private will be set to private by HMIS Administrators and the user who entered the data will be contacted to make them aware of the error and to offer additional training/support.

## 3.5 Strategies to End Homelessness (STEH), UFA, CoC Lead, and HMIS Lead

### 3.5.1 HMIS Policy Development

**Policy:** The HMIS Lead is responsible for writing Cincinnati/Hamilton County CoC's HMIS policies and procedures consistent with the current, active HMIS rules and guidelines, and in consideration of the unique needs of their partner organizations and the community.

**Procedure:**

1. Strategies to End Homelessness will draft HMIS policy documents consistent with HUD rules and guidance.
2. Draft policies will be provided to community partners and organizations for a comment period for a minimum of 30 days.
3. Responses will be replied to and/or incorporated into the final draft.
4. If significant revisions are made, the policy drafts will be returned to CHOs for a second comment period for a minimum of 10 days.
5. The final draft will be presented to the Homeless Clearinghouse for approval.
6. Policies that are not approved will be sent back to Strategies to End Homelessness for editing/re-writing.
7. Re-written policies will be provided to CHO's for a comment period for a minimum of 10 days.
8. Responses will be provided to the Clearinghouse, replied to, and/or incorporated into the final draft.
9. The revised final draft will be presented to the Homeless Clearinghouse for approval.
10. Steps 5-8 above will be repeated as needed until policy documents are approved.
11. Strategies to End Homelessness will distribute approved policies to CHOs.
12. Approved policies will be published on Strategies to End Homelessness' website.

### 3.5.2 Participant Questions and Grievance

**Policy:** Participant requests for data, questions about data, or grievances about HMIS will be deferred to the CHO who entered the data. The HMIS Lead will intervene if the CHO no longer has access to HMIS.

**Procedure for Requests for Data or Data Corrections**:

1. The HMIS Lead will instruct the participant to contact the CHO.
2. The HMIS Lead will also notify the CHO of the request and may request a copy of the CHOs grievance procedures.
3. If possible, the HMIS Lead will provide the participant with the CHO's procedure.
4. If the CHO no longer has access to HMIS:
    a. The HMIS Lead will only provide HMIS data to program participants can confirm non-identifying information entered in HMIS (such as the dates services were provided and the program name) and also present one or more of the following:
        i. A photo state ID or driver's license
        ii. Another form of identification with a photo (i.e. school ID, passport, etc.)
        iii. A social security card and birth certificate.
    b. Only data about the requesting program participant or their underage dependents will be provided.
    c. Only basic client information (available on the client profile), enrollment details, and exit details will be provided personally to the participant in paper format or as PDF documents available from a secure SharePoint drive.
5. The HMIS Lead will not modify data entered by a CHO as a result of this type of request.

**Procedure for Participant Questions**:

1. The HMIS Lead will instruct the participant to contact the CHO.
2. The HMIS Lead will also notify the CHO of the request and may request a copy of the CHOs grievance procedures.
3. If possible, the HMIS Lead will provide the participant with the CHO's procedure.
4. If the CHO no longer has access to HMIS:
    a. The HMIS Lead will answer questions about HMIS data collection standards, HMIS rules and guidelines, or HMIS policies and procedures.
    b. The HMIS Lead will not answer questions about specific data entered into the participant's record.

**Procedure for Participant Grievance**:

1. The HMIS Lead will instruct the participant to contact the CHO.
2. The HMIS Lead will notify the CHO of the request and ask for the CHO's grievance procedure.
3. If possible, the HMIS Lead will provide the participant with the CHO's grievance procedure.
4. The HMIS Lead may provide the participant with contact information for the HUD field office or the appropriate funder.

### 3.5.3 User Grievance

**Policy**: HMIS User grievances will be resolved through collaborative efforts between the CHO and the HMIS Lead.

**Procedure:**

1. The CHO PPP will report all HMIS-related user grievances to the HMIS Lead and HMIS Administrators by emailing HMISsupport@end-homeless.org or contacting the HMIS Director.
2. The HMIS Lead will contact the CHO PPP if a user reports a grievance directly to the HMIS Lead or HMIS Administrators.
3. HMIS Administrators will provide an initial response to the grievance via email within 10 days of receiving the grievance.
4. HMIS Administrators will work with the User and CHO to identify a plan for a resolution. The plan will include a timeline and action steps.
5. The CHO PPP will be included on all communications about the grievance, face-to-face or phone/virtual conversations will be summarized and sent to the CHO PPP and user.
6. The CHO PPP may contact STEH Leadership if the user is not satisfied with the resolution provided by HMIS Administrators.

**Policy**: STEH Leadership will respond to HMIS User grievances that remain unresolved by the CHO or HMIS Administrators.

**Procedure**:

1. CHO PPPs may contact Jennifer McEvilley, STEH Managing Director, jmcevilley@end-homelessness.org, if an HMIS user grievance is not addressed by HMIS Administrators.
2. Jennifer McEvilley will send an initial respond or let the CHO PPP know what STEH worker the grievance will be assigned to within 15 working days (Monday – Friday).
3. Additional communications will include action steps and timelines as needed.
4. The final resolution will be documented in writing.

### 3.5.4 HMIS Data Quality Benchmark Development

**Policy:** Cincinnati/Hamilton County HMIS Data Quality Benchmarks are developed through a collaborative process which includes input from CHOs, the HMIS Lead, UFA/CoC Lead, and other stakeholders (e.g. CoC Workgroups, Persons with Lived Experience) as defined by the Continuum of Care Policy Development policy. HMIS Timeliness Benchmarks approved by the Homeless Clearinghouse.

**Procedure:**

1. The HMIS Lead will write the initial draft of the Cincinnati/Hamilton County CoC data quality benchmarks based on collaboration with CoC stakeholders (such as the CoC Monitoring subcommittee, the CoC Clearinghouse, or other relevant workgroups).
2. Draft benchmarks will be shared with HMIS CHO PPPs for a response period. Feedback will be reviewed with the initial collaborating workgroups if needed.
3. The final draft of the data quality benchmarks will be presented to the Homeless Clearinghouse for approval.
4. Approved data quality benchmarks will be incorporated into the HMIS Policies and Procedures and made available on the Strategies to End Homelessness website.

### 3.5.5 HMIS Monitoring

**Policy**: The HMIS Lead will monitor CHOs for compliance with HMIS policies and procedures at least yearly.

**Procedure**:

1. The STEH Compliance team will schedule monitoring in advance through an email which will set expectations for the monitoring process.
2. All the CHO's HMIS programs will be monitored at the same time.
3. Results will be communicated in the monitoring report.
4. STEH will work with the CHO to correct any issues found and provide counseling to help fix organizational or management issues if needed.
5. A referral may be made to the CoC Monitoring Subcommittee for next steps if the CHO does not correct their issues, refuse STEH counseling, or the issues are serious enough to impact community-wide reporting.

## 3.6 The Homeless Clearinghouse

### 3.6.1 HMIS Policy Development

**Policy:** The Homeless Clearinghouse approves the current HMIS policy and procedure documents annually for relevance and correctness and no policy updates will be in effect until revisions have been approved.

**Explanation:** The following HMIS policy documents will be enforced and active if approved by the Homeless Clearinghouse:

- HMIS Comprehensive Policies and Procedures (including HMIS Governance Charter, HMIS Data Quality Plan, and HMIS Security Plan)
- HMIS User Agreement and Code of Ethics
- HMIS Privacy Notice and Client Consent Form

**Procedure:**

1. Final drafts of HMIS policy documents (see HMIS Policy Development, STEH) will be presented to the Homeless Clearinghouse for approval.

2. The Homeless Clearinghouse may require review by the Homeless Clearinghouse Steering Team or other working group or subcommittee before voting on approval.
3. The Homeless Clearinghouse will vote to approve the document(s).
4. The Homeless Clearinghouse will provide specific instructions for re-writing the documents if the document is not approved.
5. The document(s) will replace the previous policy document(s) after a majority of the Clearinghouse vote to approve.

### 3.6.2 HMIS Data Quality Benchmark and Policy Approval

**Policy:** Cincinnati/Hamilton County CoC Board, locally known as the Homeless Clearinghouse, will approve data quality benchmarks. Only approved data quality benchmarks, policies, and procedures will be enforceable.

**Procedure:**

1. The HMIS Lead will present a final draft of HMIS data quality benchmarks, policies, and procedures to the Homeless Clearinghouse.
2. The Homeless Clearinghouse may request they be revised before approving, in which case the HMIS Lead will restart the data quality benchmarks process until revisions requested have been integrated into the data quality document(s).
3. Data quality benchmarks and policies will be considered approved when a voting majority of the Homeless Clearinghouse votes to approve.

# 4 HMIS Data Quality Plan

## 4.1 Introduction

This HMIS Data Quality Plan is included in this document and is developed using the HMIS procedure for developing HMIS policies. It follows the rules and guidelines listed in the Homeless Management Information Systems (HMIS); Data and Technical Standards Final Notice and HUD's most HMIS Data and Technical Standards.

## 4.2 Why is Data Quality Important?

Data is important to understand homelessness, how to prevent it, and how to solve it. However, the data can only be helpful if it is of good quality.

Other benefits of entering good data:

- Save time by not needing to go back and correct the data.
- Provides good information for workers providing help to people and families.
- Helps the CoC get more money for homelessness programs and services.
- Keeps us in good standing with HUD and other federal, state, and local funders.

## 4.3 How is Data Quality Decided?

HMIS Data quality looks at how timely, valid, and correct the data in HMIS is, including:

- Is it entered quickly, in a timely manner?
- Are the questions understood the same way by users? By Participants?
- Are there mistakes in the data?
- Is the data complete? Or are there blanks? Are there answers like "Client prefers not to answer," "Client doesn't know," or "Data not collected," which counts as poor data quality?

HUD and other federal, state, and local funders mostly decide what data is collected. HMIS Administrators build out the questions and screens and provide training and support to HMIS users so they understand how to enter the data. CHOs monitor the data quality for their programs and ask users to correct data when needed. HMIS Administrators may monitor for additional data quality checks to guide HMIS training updates. Users or CHO PPPs may be requested to correct these data issues.

Users and CHOs may request more support from HMIS Administrators if they need help to improve their data quality.

## 4.4 Data Quality Benchmarks

The CoC's overall goal is to collect 100% of all data, correctly, and in real time. However, that is not possible in every case. Therefore, the HMIS data quality benchmarks are the goals agreed to through the HMIS Data Benchmark Development process. CHOs may request these Benchmarks be reviewed at any time.

**Incentives and Consequences:** CHO data quality will be reviewed during Annual Monitoring by STEH Compliance. Data quality may also be considered in the Cincinnati/Hamilton County scoring process. Projects that meet data quality benchmarks may be awarded more points while projects which fail to meet data quality benchmarks may lose scoring points. This scoring point system is used to determine competitiveness for funding renewal projects. Scoring criteria are determined annually in accordance with the Cincinnati/Hamilton County Scoring Subcommittee.

### 4.4.1 Timeliness

**Data import considerations:** Date entered is an element that is imported from the source database into the HMIS database, therefore, timeliness factors should not be affected by importing data into HMIS.

#### *4.4.1.1 Timeliness Benchmarks*

| **Benchmarks for intake and exit records entered beyond the 3-day standard by project type** | | | | |
|---|---|---|---|---|
| | Intake records for all projects (PSH, RRH, TH, HP/Diversion, ES, ES NBN, SO/SSO, SH) | Exit records for all projects (PSH, RRH, TH, HP/Diversion, ES, ES NBN, SO/SSO, SH) except Winter Shelter exit | Exit Records for Winter Shelter | Exit Records for non-HUD SO |
| 4-6 days | 5% | 5% | N/A | N/A |
| 7-10 days | 3% | 3% | N/A | N/A |
| 11+ days | 0% | 0% | N/A | N/A |

### 4.4.2 Accuracy and Completeness

All data elements should be entered fully and completely whenever possible. A Status Update assessment should be completed at least monthly whenever a participant's situation changes. (For example, if a person's income or health benefits change). An Annual Assessment must be completed within 30 days before to 30 days after the participant's project start date anniversary for any participant who is active in a project for 1 year or longer. For families, the entire family will need an Annual Assessment within 30 days before to 30 days after the head of household's project start date anniversary. Data not entered, entered incompletely (including "client prefers not to answer", "Client doesn't know", or "Data no collected"), incorrectly, or entered outside of the Annual Assessment timeline will be excluded from important reports and may affect funding.

#### *4.4.2.1 Accuracy and Completeness Benchmarks*

**Personally Identifiable Information (PII)**

| **Benchmarks for unknown (don't know/refused) and missing/data issues responses for all project types (PSH, RRH, TH, HP/Diversion, ES, ES NBN, SSO/SO, SH)** | | |
|---|---|---|
| Data Element | Client Doesn't Know/Client Prefers Not To Answer | Information Missing/Data Issues |
| 3.1 Name | 0% | 0% |
| 3.2 Social Security Number | 1% | 1% |
| 3.3 Date of Birth | 0% | 0% |
| 3.4 Race | 0% | 0% |
| 3.5 Ethnicity | 0% | 0% |
| 3.6 Gender | 0% | 0% |

**Universal Data Elements**

| Benchmarks for all project types (PSH, RRH, TH, HP/Diversion, ES, ES NBN, SSO/SO, SH) | |
|---|---|
| Data Element | % Error rate |
| 3.7 Veteran Status | 0% |
| 3.10 Project Start Date | 0% |
| 3.15 Relationship to Head of Household | 0% |
| 3.16 Client Location | 0% |
| 3.8 Disabling Condition | 1% |

**Program Specific Data Elements**

| Benchmarks for error rates by project type | | | | | | | |
|---|---|---|---|---|---|---|---|
| Data Element | PSH, HP | RRH, TH | ES, SO/SSO | ES NBN | SH | Non-HUD Housing Projects | Non-HUD ES, SO/SSO |
| | % Error rate | % Error rate | % Error rate | % Error rate | % Error rate | % Error rate | % Error rate |
| 3.12 Destination | 0% | 0% | 3% | N/A | 0% | 0% | 3% |
| 4.2 Income and Sources at Start | 0% | 0% | 0% | 0% | 0% | N/A | N/A |
| 4.2 Income and Sources at Annual Assessment | 5% | 10% | 0% | 0% | 0% | N/A | N/A |
| 4.2 Income and Sources at Exit | 0% | 0% | 0% | N/A | 0% | N/A | N/A |
| 4.3 Non-Cash Benefits at Start | 0% | 0% | 0% | 0% | 0% | N/A | N/A |
| 4.3 Non-Cash Benefits at Annual Assessment | 5% | 10% | 0% | 0% | 0% | N/A | N/A |
| 4.3 Non-Cash Benefits at Exit | 0% | 0% | 0% | N/A | 0% | N/A | N/A |

**Chronic Homeless Data Elements**

| Benchmarks for Records Missing Information Needed to Calculate Chronic Homelessness |
|---|

| Data Element | PSH, RRH, TH, ES, ES NBN, SO |
|---|---|
| % of records unable to calculate | 0% |

**Inactive Records**

| Benchmarks for Inactive Records | |
|---|---|
| Data Element | SO, ES NBN |
| | % of Inactive Records |
| Contact (Adults and Heads of Household in Street Outreach or ES-NbN | 0% |
| Bed Night (all clients in ES-NbN) | 0% |

**Accuracy (No benchmarks proposed at this time)**

| Benchmarks for Income Records in HMIS Inconsistent with Income Documentation in Participant Record | |
|---|---|
| Data Element | PSH, RRH, TH, HP/Diversion, ES, ES NBN, SO/SSO, SH |
| | # Error Count |
| Income entries inconsistent with documentation in client file | |

**Client Release of Information - Additional Data Quality Element Considerations (No benchmarks proposed at this time)**

| Benchmarks for Participant Records Missing Releases of Information | | |
|---|---|---|
| Data Element | PSH, RRH, TH, HP/Diversion, ES, ES NBN, SO/SSO, SH | |
| | Error Count | % Error Rate |
| Active participant records missing ROIs at the time of monitoring | | |
| Participant records missing ROIs in the 12 months preceding the monitoring | | |

## 4.5 Additional Data Quality Concerns

Users will document services provided to participants through a CHOs HMIS programs as needed by the CHO, required by funders or regulations, or as included in HMIS training courses and support documentation.

Some HMIS or CoC processes may require additional data entry requirements beyond the HUD required data elements. These data points and processes are critical to Coordinated Entry documentation, required by non-HUD funders, or critical for other requirements within the HMIS.

# 5 HMIS Privacy Plan

## 5.1 Introduction

CHOs and the HMIS Lead are responsible for complying with the minimum requirements listed in the Homeless Management Information Systems (HMIS); Data and Technical Standards Final Notice related to privacy, limits on data collection, data quality, limits on data use, access to correction, and accountability. A CHO may adopt privacy protections that exceed the baseline requirements for each area.

The HMIS Privacy Notice and Client Consent Form describes how participant's information may be used and shared, how participants can get access to their information, and makes sure all CHOs are held to the same minimum standards. It is the foundation of this privacy plan. It is each CHOs' responsibility to make sure its own policies and practices are in line with the full extent of HUD's rules and regulations and comply with any other federal, state, and local laws that apply to them.

## 5.2 CHOs Covered Under HIPAA

When a CHO is a Health Insurance Portability and Accountability Act (HIPAA) covered organization, the provider is required to operate in accordance with HIPAA rules. The Final Notice states that such a provider is not required to comply with the HMIS privacy or security standards. Exempting HIPAA covered organizations from the HMIS privacy and security rules avoids all possible conflicts between the two sets of rules. CHOs not covered under HIPAA are subject to the HMIS privacy and security standards. CHOs are also responsible to know what applicable state and local privacy laws apply to them. (REF : https://www.federalregister.gov/d/04-17097/p-526)

It is possible that part of a CHO's operations may be covered by the HMIS standards while another part is covered by the HIPAA standards. CHOs' describe their own privacy and security requirements in their own policy documents. This should include what information is held to the HIPAA standards and what information is held to the HMIS standards. This is to make sure program participants understand the rules around their data privacy and security.

## 5.3 Participant Rights and Consent

Program participants have the right to consent to share data with other CHOs. Sharing data between CHOs can help:

- Improve access and provide quality services.
- Coordinate referrals for housing or services such as food, utility help, counseling, etc.
- Reduce the need to repeat their story to every service provider.
- Provide information needed to match to a housing provider (if available).

Program participants may choose not to share data in HMIS with other CHOs. HMIS users must review the HMIS Privacy Notice and Client Consent Form with participants to make sure participants understand their rights and how their data will be used. HMIS users must know how to set specific records or data elements to private when a participant chooses not to share information in HMIS with other CHOs. Data entered into HMIS will be shared broadly with other CHOs unless it is set to private by HMIS users.

Participants, at a minimum, have a right to:

- Review their PPI/PII as entered in HMIS.
- Request corrections to that data.
- Request that specific data elements will be set to private and not shared outside of the CHO entering the data other than for the purposes outlined in the HMIS Uses and Disclosures.

CHOs may choose to provide additional information to participants including enrollment detail, services provided, referrals made, and notes.

CHOs may deny a participant review of their data if:

- The data is reasonably expected to be used in a legal proceeding.
- Providing the data includes data from another source that expects it to be private and not shared.
- The data includes information about another person.
- Providing the data is reasonably likely to be used to threaten or create an unsafe situation for any person.

A CHO can reject repeated or harassing requests to view or correct data. A CHO that denies an individual's request to review or correct data must explain the reason for the denial to the individual and must document the request and the reason for the denial in the participant's record. (ref: https://www.federalregister.gov/d/04-17097/p-578)

## 5.4 HMIS Uses and Disclosures

### 5.4.1 Allowable Uses and Disclosures of PPI/PII

CHOs, HMIS Users, the CoC, the HMIS/CoC Lead, System Administrators (including the HMIS and HMIS vendor staff), and HMIS users may have access to PPI/PII and have responsibilities to keep this information private. However, this data is collected for and may be used for specific reasons. This section provides guidance on when and how PPI/PII may be used or shared and to balance competing interests in a responsible and limited way. *(Ref.* https://www.federalregister.gov/d/04-17097/p-528*)*

i. A CHO and a CHO's HMIS users may only share or use PPI/PII entered by the CHO unless data entered by another CHO is used to facilitate services or confirm eligibility to receive services.
ii. System Administrators (including support staff from the HMIS vendor) may use PII when supporting the HMIS including providing user support, making sure the system and reports are working as expected, and to correct duplicate records.
iii. The HMIS and CoC Lead may use PII to monitor data correctness and compliance with contracts. And for research to identify gaps in the homeless system, identify additional funding and services to help people experiencing homelessness, find ways to improve services for people experiencing or at risk of homelessness, and other work related to ending homelessness in our community.
iv. The CoC, through CoC appointed workgroups, to review individual cases in a collaborative setting and identify steps to improve their situation.
v. PPI/PII may be used to:
    a. Provide or coordinate services to an individual or family.
    b. Report to funders or other functions related to payment to the CHO for services provided.
    c. Functions related to managing or running the CHO and the CHO's projects, including but not limited to legal, audit, monitoring, and oversight.
    d. Functions related to making sure the data is correct and the HMIS is performing as intended.
    e. To prevent a serious threat to health or safety:
        - The CHO must believe in good faith sharing the PPI/PII will lessen or prevent a serious threat to the health or safety of a person or the public.

- And the data is shared with a person who is reasonably able to prevent the threat (including the target).

f. If the CHO reasonably believes the person is a victim of abuse, neglect, or domestic violence:
   - And is required by law to report the neglect, abuse, or domestic violence.
   - Or the person agrees for the CHO to report the neglect, abuse, or domestic violence.
   - The CHO should tell the person whose PPI/PII was shared unless telling that person would put them in harm or if that person is responsible for the abuse, neglect, or violence.

g. When required by law:
   - CHOs should only share data that is specifically required.

h. For law enforcement purposes:
   - When required by a lawful court order, warrant, subpoena, or summons.
   - If the CHO reasonably believes in good faith the PPI/PII is evidence related to a crime that occurred on the premises of the CHO.
   - Name, date of birth, place of birth, social security number or description may be shared, at the CHO's discretion to help officials locate a suspect, fugitive, witness, or missing person.
   - Specific information needed by the US Marshalls or other appropriate federal officers to help protect the US President, foreign leaders, or others under the jurisdiction of the federal officers. *(Ref: 18 U.S.C. 3056, 18 U.S.C. 871 and 879)*.
   - In response to an official written request by a law enforcement official if:
     - The request is signed by a supervisor from the law enforcement agency.
     - The request includes detail about the legitimate investigatory reason the information is needed.
     - The requested information is limited to what is reasonable for the investigatory reason stated.
     - The request provides a reason why PPI/PII is required and why non-identifiable information could not be used.

i. For research purposes:
   - The researcher(s) must be approved and have a formal written agreement with the CHO providing the data.
   - The written research agreement must be approved in writing by an administrator of the CHO providing the data.
   - The written agreement must include:
     - Rules and limitations for the security and processing of the data.
     - How data will be returned or properly disposed of when the research project is finished.
     - Limit how the data will be used.
     - Require the researcher(s) to agree to and follow the terms and conditions of the agreement.

### 5.4.2 Uses and Disclosures for Shared Data

Shared data refers to data entered by one CHO which is made available to another CHO through the participant's HMIS record. CHOs and HMIS Users who access shared data agree to:

1. Only access participant records for a specific business purpose (such as to provide services to that participant/household, monitor the data for supervision or oversight, in order to provide user support or identify data entry errors, research for a specific, approved purpose, etc.).

2. Maintain the confidentiality of the shared data to the same extent as is required for data entered by their users.
3. Users will only delete, edit, or modify data entered by their CHO.
4. Implement all measures required to safeguard data entered by their users to the shared data.
5. Shared data will be used solely for the purposes of trauma informed care, informed services provision, or collaboration with the other CHOs/projects to benefit specific participants or households.
6. Only data entered by their users will be used for strategic purposes such as reporting outcomes. No CHO will use, publish, or share data entered by another CHO for strategic purposes or reporting comparisons or outcomes without prior approval from the CHO who entered the data.
7. The CHO agrees to comply with all applicable laws, regulations, and ethical standards governing the use and sharing of data.

## 5.5 Limits on Data Collection

A CHO may collect participant PPI/PII only when data is used for the purpose it was given or when required by law. HMIS users will only collect or access participant data needed to provide services to that participant/household. A CHO must collect PPI by lawful and fair means and, where appropriate, with the knowledge or consent of the individual. A CHO must post a sign at each intake desk (or comparable location) that explains generally the reasons for collecting this information. The HMIS Privacy Notice and Client Consent Form can be used for this purpose if it accurately reflects the CHO's policies and procedures. *(Ref: HMIS Data and Technical Standards Final Notice 4.2.1)*

# 6 HMIS Security Plan

## 6.1 What is Security?

Security is the amount of protection available to prevent people not approved from accessing HMIS data. The security of the data held in and outside the HMIS database is a high priority in the community. People who access HMIS data, either through HMIS or outside of HMIS, must take the privacy and security of all HMIS information seriously. This plan aims to protect HMIS data from security threats or hazards and make sure HMIS users understand and follow these security standards.

CHOs may commit to additional security protections consistent with HMIS requirements by applying hard copy security provisions to paper and hard copy information that is not collected specifically for the HMIS.

## 6.2 Application Security

The HMIS Lead will ensure that HMIS processes and software application meets security provisions required by HUD, including:

- A user authentication system consisting, at a minimum, of a username and a password. And those passwords are required to meet the reasonable industry standard requirements.
- HMIS data is encrypted during transmittal and at rest.
- The HMIS system contains user audit logs pertaining to participant data.
- The HMIS vendor institutes security process including physical server infrastructure and security audits.
- HMIS system data is limited to trained, authorized users.

## 6.3 Hard Copy Security

Paper or other hard copy containing PII that is either generated by or for HMIS must be kept secure:

- Supervised and managed so the data is not easily viewed by others (i.e. kept in a folder or covered when viewable by others) when in publicly accessible areas.
- Secured in area(s) that are not accessible by the public when not in use (locked in a secure cabinet, room, or drawer).
- Hard copy PII no longer in use should be shredded or burned.

**Remote work considerations:** Staff working remotely are required to supervise paper or hard copy PII generated by or for the HMIS when in use and secure hard copy PII in a locked location (a locked drawer, room, or briefcase). Hard copy PII no longer in use should be shredded or burned.

## 6.4 Physical Access, Hardware, Software, and Connectivity

HMIS Administrators will allow only approved and trained users to access the HMIS software. All users will be required to read, sign, and agree to follow the HMIS User Agreement and Code of Ethics before accessing program participant data. Beyond this, all CHOs and HMIS users are expected to follow these additional security measures.

Note: A high publicly trafficked area would include areas where non-employees frequent. A low publicly trafficked area would include areas where non-employees are supervised or areas where employees without HMIS access can access. Although requirements are less stringent for low publicly traffic areas, it is still important that users are aware of their surroundings and reduce the potential for inadvertently sharing sensitive information.

### 6.4.1 Physical access

i. Ensure workstations are located where they are not easily viewed by the public (located in areas where there is low public traffic or in such a way that screens cannot be viewed from high public traffic areas).
ii. Computers in public areas should be immediately locked with a password protected screen or turned off when not in use, staff are not present, or if viewable by unauthorized persons.
iii. Enable an automatic password protected screen saver or automatically log users off if the system has remained dormant for a maximum 15 minutes and the computer is in a publicly highly trafficked area or a maximum of 30 minutes for workstations placed in low publicly trafficked areas.
iv. Power off workstations when not in use for an extended period of time. Consider enabling an automatic computer shut down if it has remained dormant for 2 hours.
v. Consider physically locking computers that are located in public areas so they cannot be physically removed.
vi. Users should log off Clarity when not in use.
vii. Usernames and passwords must never be shared or kept in a location where they can be accessed by others.
viii. Users should not save their HMIS username and password to their browser.

**Remote work considerations:** Staff working remotely are required to be diligent to avoid mistakenly sharing HMIS data.

- Move computer screens so that the content is not easily viewed by others.
- Identify strategies to quickly conceal HMIS data so it cannot be viewed by other people (e.g., quickly lock your computer using keyboard shortcuts, or use “lid” configuration settings to lock when laptop lid is closed).

### 6.4.2 Hardware, Software, and Connectivity

System security provisions must be applied to all the systems where personally identifying information generated either by or for the HMIS is stored, including, but not limited to, networks, desktops, laptops, and servers.

i. Each workstation used to access HMIS or store data for or from the HMIS must include up to date virus protection and firewall protection.

ii. Any server or network used to access HMIS or store data for or from HMIS must include up to date virus protection and firewall protection.
iii. Any workstation, server, or network used to access HMIS or store data for or from HMIS must include at a minimum password protection.
iv. Workstations/devices accessing HMIS must have the most up-to-date version of an HMIS supported web browser to ensure the latest security features are in place. [Supported Web Browsers for Accessing Clarity Human Services (bitfocus.com)]
    - Google Chrome
    - Microsoft Edge
    - Mozilla Firefox
    - Apple Safari
v. Delete all data from data any computer, server, CD, thumb drive, or other medium which contains participant level HMIS data and reformat the storage medium more than once before reusing or disposing of the medium.

**Remote work considerations:**

- Only use secure networks or hot spots, never work in HMIS or with HMIS data on a public network.
- Save HMIS data to a secure server; never to your personal or work-computer.
- When working from home, reboot the home router or modem to improve performance and ensure your internet provider maintains the most current network security.
- Users may use a personal VPN for an extra layer of protection.

## 6.5 Disaster Protection and Recovery

The HMIS Lead must confirm the following baseline disaster and recovery requirements are met for the HMIS.

- System redundancy allows HMIS data to be recovered in case of a disaster.
- The system and data held within the system are stored in a secure location with the appropriate temperature controls, fire suppression systems, and surge protections.
- Data disposal protocols.
- Protocols for communication with staff, the CoC, and CHOs in case of a disaster.
- Annual security review.

## 6.6 Security Breaches

A security breach occurs when any person with access to HMIS data allows that data to be viewed or used, either intentionally or unintentionally, by a person not approved to view or use the data. This can include unauthorized access to HMIS by sharing passwords, leaving computers unattended, or saving usernames and passwords to a browser. It can also include:

- Printed data being left unsecured so it can be viewed by unauthorized people.
- Discussing verbally in places where the discussion can be overheard by unauthorized people.
- Storing or sending data electronically in a way it can be accessed by unauthorized people.

This security policy is intended to provide procedures to protect the data in HMIS. This Security Breaches policy is intended to address how the CHOs and HMIS Lead will respond when a breach occurs, including: assessing the incident, minimizing the damage, ensuring rapid response, and documenting and preserving evidence.

### 6.6.1 Notification of a Security Breach

1. CHOs or HMIS Users will inform STEH HMIS Administrators of any breach of the privacy and security policies outlined in this document, the HMIS User Agreement and Code of Ethics, The HMIS Privacy Notice and Client Consent Form, or the HUD Data and Technical Standards as soon as possible.
2. STEH HMIS Administrators will notify the HMIS User and CHO PPP of any type of security breach they are made aware of as soon as possible.

### 6.6.2 Security Breach Levels, Responses, and Remedies

While all security breaches are serious, these levels of security breaches take into consideration several factors when determining how the breach will be addressed. The HMIS Lead and CHOs will work together to address security breaches and improve the security of HMIS data.

#### *6.6.2.1 Low Level Security Breaches*

Low – At the low-impact level, data breaches typically have minimal adverse effects on a CHO. The compromised information might not significantly impact operations, privacy, or the CHO's reputation. However, this does not imply that low-impact data should be overlooked or left unsecured.

For example: Participant PII is inadvertently shared through a means that is assumed to be secure by the user (e.g. sending PII through email or email attachments, accessing PII while your screen can be viewed by CHO staff who are not authorized to view client PII).

- Users and CHOs determined to engage in a low-level security breach will be notified by HMIS Administrators or the HMIS Lead including corrective action for the current breach or to make sure the breach does not occur again.
- If multiple low-level breaches occur for a specific CHO, HMIS Administrators and the CHO will work together to develop a plan to improve security which may include but is not limited to additional training provided by the HMIS Lead and additional monitoring provided by the CHO.

#### *6.6.2.2 Moderate Level Security Breaches*

Moderate - With moderate impact, the stakes are higher. Breaches involving this level could lead to repercussions, affect trust, or breach compliance requirements.

For Example: Participant PII is left unsecured or data is accessed by people who have the participants implied or direct consent to the data but are accessing the data in an unsecured manner. (For example, users have been approved to access PII and have permission to access PII based on the participant directly providing PII but are accessing the system using another user's username and password, PII is kept in a closed but unlocked drawer or filing cabinet)

- User's access will be temporarily terminated for users determined to engage in a moderate-level security breach.
- The HMIS Lead and CHO will work with work together to investigate the breach, determine all parties associated with the breach and an appropriate course of action for correction.
- Additional parties potentially associated with the breach may also have their access temporarily terminated while the breach is investigated.
- Corrective action may include but is not limited to additional training for the user(s) and other involved staff and additional monitoring of involved staff.

- Corrective action may include permanent removal of a user's access to HMIS or a user's access may be reactivated once the CHO and HMIS Lead agree the corrective action has been completed.

#### *6.6.2.3 High Level Security Breaches*

High - The highest data impact level carries the most severe consequences. A breach involving high-impact can have effects on CHOs, including possible financial losses, legal ramifications, and damage to its reputation. To safeguard this critical information, CHOs must guarantee the highest level of security controls, continuous monitoring, and incident response protocols.

For example: Intentional disregard of the HMIS policy and procedures regarding consent, privacy, and security (For example, sharing HMIS usernames and passwords with people who are not approved to access HMIS, leaving PII and/or health related information in publicly accessible areas, leaving HMIS open and available on unsecured and unattended computers in publicly accessible areas)

- User's access will be temporarily terminated for users determined to engage in a high-level security breach.
- The HMIS Lead will work with work together with the CHO to investigate the breach and determine all parties associated with the breach.
- Additional parties potentially associated with the breach may also have their access temporarily terminated while the breach is investigated.
- The HMIS Lead and CHO will work together to determine corrective actions.
- Corrective action may include permanent termination of HMIS access for involved staff.