Coalition for the Homeless
2000 Crawford, Suite 700
Houston, TX 77002
Tel: 713-739-7514

Homeless Management Information System (HMIS)

Policies and Procedures

TX-700 Continuum of Care

CONTACT INFORMATION

Website information on Houston/Harris County HMIS:
https://www.cfthhouston.org/hmis-v2

The HMIS team provides ongoing assistance to all participating agencies. An agency can request additional training or onsite visits from the HMIS staff at any time:
https://www.cfthhouston.org/hmis-v2#HMISUserTrainings

ClientTrack Training Website:
https://clienttrack.eccovia.com/login/HC_Harris_Train

ClientTrack Production Website:
https://clienttrack.eccovia.com/login/HC_Harris

HMIS help desk:
hmis@cfthhouston.org

For all issues related to HMIS & ClientTrack submit a ticket to IssueTrak:
https://hmissupport.homelesshouston.org

Table of Contents

I. BACKGROUND AND STRUCTURE 4

A. Introduction 4

B. History 4

C. Federal Reporting 5

1. System Performance Measures (SPM) 5

2. Annual Homeless Assessment Report and Longitudinal System Analysis (AHAR and LSA) 5

3. Housing Inventory Count (HIC) 6

4. Point in Time (PIT) Count 6

II. ROLES AND RESPONSIBILITIES 7

A. Coalition for the Homeless (CFTH) – HMIS Responsibilities 7

B. Participating Agency Responsibilities 8

III. IMPLEMENTATION POLICIES AND PROCEDURES 8

A. HMIS Agency Participation Agreement 8

B. HMIS User License Agreement 8

C. Data Collection Requirements 8

D. Protecting Privacy Information 9

E. HMIS Data Standards Terms and Concepts 10

F. HMIS Project Start and Exit Date 11

G. HMIS Support Protocol 12

H. HMIS Fees 12

IV. SECURITY POLICIES AND PROCEDURES 12

A. Protecting Personally Identifiable Information (PII) 12

B. Training 14

C. User Authentication 15

D. Passwords 15

E. Hardware Security Measures 16

F. Security Violations and Sanctions 16

G. Equal Access 16
V. DATA POLICIES AND PROCEDURES 16
A. Data Quality 16
1. Data Timeliness 16
2. Data Completeness 16
3. Data Accuracy 16
B. Preventing Client Duplication at Program Entry 17
C. Data Use and Disclosure 17
D. Data Release 18
E. Custodian of HMIS Records 18
VI. CLIENT CONSENT, PRIVACY AND RIGHTS 18
A. Client Consent 18
B. Client Privacy 18
C. Client Grievance 19
VII. APPENDICES 21

I. BACKGROUND AND STRUCTURE

A. Introduction

A Homeless Management Information System (HMIS) is a database used to record and track client-level information on the characteristics and service needs of homeless persons. An HMIS ties together homeless service providers within a community to help create a more coordinated and effective housing and service delivery system.

The U. S. Department of Housing and Urban Development (HUD) and other planners and policymakers at the federal, state and local levels use aggregate HMIS data to obtain better information about the extent and nature of homelessness over time. Specifically, an HMIS can be used to produce an unduplicated count of homeless persons, understand patterns of service use, and measure the effectiveness of homeless programs.

In addition to serving as the lead agency for TX-700 Continuum of Care's (CoC), the Coalition for the Homeless is also as the HMIS Lead. As the HMIS lead we are the entity designated by the Continuum of Care in accordance with the HMIS Proposed Rule (24 CFR Part 580) to operate the Continuum's HMIS on the Continuum's behalf. The TX-700 Continuum of Care's (CoC) HMIS is staffed at the Coalition for the Homeless. The Coalition's HMIS staff is responsible for the administration of the HMIS software and providing technical assistance to participating agencies and end-users.

Agencies that participate in the TX-700 CoC's HMIS are referred to as "participating agencies." Each participating agency needs to follow certain guidelines to help maintain data privacy and accuracy. The guidelines listed in this document do not replace the more formal and legally binding agency agreement that each agency signs before program implementation.

B. History

In 2001, Congress instructed the U.S. Department of Housing and Urban Development (HUD) to take measures to improve available data concerning homelessness in the United States. In response, HUD mandated all Continuum of Care regions to implement region-wide databases that would allow an unduplicated count of clients served. Out of this directive came the Homeless Management Information System (HMIS), a computerized data collection application that facilitates the collection of information on homeless individuals and families using residential or other homeless assistance service agencies and stores that data in a centralized database for analysis.

In 2004, HUD published the HMIS Data and Technical Standards Final Notice which describes the types of data that HUD funded providers must collect from clients receiving homeless assistance services. The notice also presented privacy and security standards for providers, CoCs and all other entities that use or process HMSI data. These data standards have been revised several times; more recently in May 2023. The revised data standards can be found at the following link: FY 2024 HMIS Data Standards Manual (hudexchange.info)

C. Federal Reporting

Having access to HMIS represents a strategic advantage for service providers. The HMIS software we use allows multi-level client data sharing between organizations, as well as client case coordination and electronic referrals. Our locally developed information-sharing model can prevent service duplications and enable collaboration between various homeless service providers, while limiting access to sensitive data. Client privacy is very important to us.

In addition to the standard data collection and reporting functionalities, the HMIS software includes a comprehensive case management module, bed management, performance measurement tools, ad-hoc reporting, software customization options, etc.

Lastly, providers already in HMIS are better positioned to apply for future funding opportunities, as many national and local funders now require HMIS participation.

1. System Performance Measures (SPM)

The McKinney-Vento Homeless Assistance Act, as amended, focuses on viewing the local homeless response as a coordinated system of homeless assistance options as opposed to homeless assistance programs and funding sources that operate independently in a community. The Act now requires communities to measure their performance as a coordinated system, in addition to analyzing performance by specific projects or project types.

The Act has established a set of selection criteria for HUD to use in awarding CoC funding that require CoCs to report to HUD their system-level performance. The intent of these selection criteria is to encourage CoCs, in coordination with ESG Program recipients and all other homeless assistance stakeholders in the community, to regularly measure their progress in meeting the needs of people experiencing homelessness in their community and to report this progress to HUD. Specifically, the SPM assess the CoC's performance against the following measures:

- Measure 1: Length of Time Persons Remain Homeless
- Measure 2: The Extent to which Persons Exiting Homelessness to PH Destinations Return to Homelessness
- Measure 3: Number of Homeless Persons: Change in PIT and Annual Counts
- Measure 4: Employment and Income Growth for Homeless Persons in CoC Program-funded Projects
- Measure 5: Number of persons who become homeless for the 1st time
- Measure 7: Successful Placement from Street Outreach and Successful Placement in or Retention of PH

2. Annual Homeless Assessment Report and Longitudinal System Analysis (AHAR and LSA)

Congress has directed the U.S. Department of Housing and Urban Development (HUD) to assist local jurisdictions in implementing an HMIS and in using data from these systems to obtain an unduplicated count of homeless persons, analyze local patterns of services usage, and assess local service needs.

The AHAR uses aggregate HMIS data from communities across the country, as well as information from CoC applications, to produce a national report on homelessness to the U.S. Congress. The AHAR is designed to:

- Develop an estimate of the number of homeless persons nationwide;
- Estimate the number of persons receiving assistance in permanent supportive housing (PSH);
- Create a descriptive profile of homeless persons and persons in PSH;
- Understand service use patterns; and,
- Estimate the nation's capacity to house homeless persons.

The AHAR to Congress is the only source of data that is available annually on the extent and nature of homelessness nationwide. As such, the LSA submission from your CoC is critical to providing federal and local policymakers with a deeper understanding of who is homeless and how homelessness changes over time. This information can be used to inform the public and help policymakers craft appropriate intervention strategies to prevent and end homelessness in the United States. Indeed, LSA data used in the AHAR will assist in tracking progress against the federal strategic plan to prevent and end homelessness.
Houston is currently a contributing state for the AHAR and has been since 2005. The AHAR is based on an unduplicated count of persons within each community, and focuses on persons who use emergency shelters, transitional housing programs and/or permanent supportive housing. The AHAR does not account for homeless persons who only use supportive service programs or are service resistant and do not access any type of homeless residential programs during the study period.

3. Housing Inventory Count (HIC)

The Housing Inventory Count (HIC) is designed to be an accurate reflection of each CoC's capacity to house homeless and formerly homeless individuals and families. It collects information about beds and units in each Continuum. The inventory is categorized by five (5) program types: Emergency Shelter, Transitional Housing, Permanent Housing, Rapid Re-housing, and Safe Haven. Whether or not they actively participate in the CoC, all residential projects, both HUD funded and non-HUD funded are to be included in this annual count. This count does exclude the following from its inventory: substance abuse facilities, foster care or group homes, incarceration facilities, and medical facilities.

4. Point in Time (PIT) Count

Point in time (PIT) counts are a critical source of data on the number and characteristics of people who are homeless in the United States. Per the HUD CoC program rules identified in 24 CFR 578.7(c)(2), this CoC participates in both the street and shelter counts. The data captured during the annual PIT count are provided to Congress as part of the AHAR. It serves to provide Congress, HUD, other federal departments, and the general public a complete understanding to the nature and extinct of homelessness. PIT count data and CoC efforts to produce an accurate count also play a critical role in the annual CoC program competition. In addition to informing HUD funding

decisions and national priorities, PIT count data are an extremely important source for local program and system planning. The sheltered and unsheltered count must be conducted during the last 10 days in January and represent all homeless persons who were sheltered and unsheltered on a single night during that period. While the unsheltered count is comprised of information gathered from homeless persons on the street on the night of the count, ALL sheltered data is taken directly from the HMIS.

II. ROLES AND RESPONSIBILITIES

The goals of our CoC's HMIS Project are to:

1. Assist homeless persons to navigate homeless service programs in Houston, Harris County, Ft. Bend County, Montgomery County, Baytown and Pasadena
2. Assist homeless service agencies with information allowing them to serve their clients better
3. Gain a greater understanding of the numbers and characteristics of the homeless population
4. Identify the needs of the homeless, both met and unmet
5. Track available resources
6. Provide information on services the homeless people receive as well as monitor outcomes and program performance
7. Increase community awareness and understanding of issues related to homelessness

To achieve these goals, we all have a role to play and responsibilities and standards to adhere to.

A. Coalition for the Homeless (CFTH) – HMIS Responsibilities

1. Execute HMIS participation agreements;
2. Monitor compliance with applicable HMIS standards on a regular basis;
3. Establish and review End User Agreements;
4. Maintain and update as needed the files for HMIS software to include software agreements, HUD Technical Submissions, HUD executed agreements and Annual Progress Reports;
5. Develop and maintain HMIS agency files to include original signed participation agreements, original signed user license agreements and all other original signed agreements pertaining to HMIS;
6. Develop and update as needed a Data Quality Plan;
7. Review and update HMIS Privacy Policy yearly;
8. Develop and review the HMIS Security Plan annually;
9. Review and update as needed the HMIS Policies and Procedures;
10. Provide copies of the Data Quality Plan, Privacy Policy, Security Plan and Policies and Procedures to the HMIS Support Committee for review and feedback on an annual basis;
11. Review national, state and local laws that govern privacy or confidential protections and make determinations regarding relevancy to existing HMIS policy;
12. Provide new user training and refresher user training monthly;
13. Pro-actively contact new users for immediate follow-up and issuance of username and password to access HMIS to begin entry of data as soon as possible following training;
14. Provide technical support to agencies using HMIS for troubleshooting and data input;

15. Oversee HMIS data and bed lists on an ongoing basis to ensure that participating agency programs are using HMIS accurately;
16. Assist agencies upon request for additional on-site training and support; and
17. Conduct an annual unduplicated count of homeless people.

B. Participating Agency Responsibilities

1. Must comply with all applicable agreements;
2. Execute and manage HMIS User License Agreements with all staff who have HMIS access;
3. Comply with the HMIS Standards as appropriate;
4. Accurately enter all required data into the HMIS system, including accurate and timely information into housing, where applicable; and
5. Each participating agency must designate an organization Security Officer and a backup Security Officer responsible for the oversight of all personnel that generate or have access to client data in the HMIS to ensure adherence to the policies and procedures described in this document
6. Attend annual HMIS security training

III. IMPLEMENTATION POLICIES AND PROCEDURES

A. HMIS Agency Participation Agreement

The Executive Director of any Participating Agency shall follow, comply, and enforce the HMIS Agency Participation Agreement (Appendix A). The Executive Director must sign an HMIS Agency Participation Agreement before granted access to HMIS. Signing of the HMIS Agency Participation Agreement is a precursor to training and user access.

1. An original signed HMIS Agency Participation Agreement must be presented to the HMIS staff before any program is implemented in the HMIS.
2. After the HMIS Agency Participation Agreement is signed, the HMIS staff will train end users to use HMIS.
3. A username and password will be granted to end users after required training is completed.

B. HMIS User License Agreement

End user of any Participating Agency shall follow, comply, and enforce the HMIS User License Agreement (Appendix B). Before given access to HMIS, the end user must sign an HMIS User License Agreement.

1. The HMIS staff will provide the end user a HMIS User License Agreement for signature after completing required training.
2. The HMIS staff will collect and maintain HMIS User License Agreements of all end users.
3. A username and password will be granted to end users after the required training is completed.

C. Data Collection Requirements

At a minimum. HUD requires that the CoC collect project descriptor information in the HMIS for all participating projects and residential projects, regardless of participation, in the served jurisdiction. The following project descriptor data elements (PDDE) are required for setup in HMIS:

1. Organization information
2. Project information

3. Continuum of Care information
4. Funding sources
5. Bed and unit inventory information

The HMIS Data Standards are comprised from a variety of resources stretching across multiple federal partners. While each of these partners require some different level of data collection, there is one set of universally required data elements.

This basic set of universal data elements (UDEs), set forth in the FY 2024 HUD HMIS Data Standards Manual, is required of all agencies. They are as follows:

- Name
- Social Security Number
- Date of Birth
- Race and Ethnicity
- Veteran Status
- Disabling Condition
- Project Start Date
- Project Exit Date
- Destination
- Relationship to Head of Household
- Client Location
- Housing Move-In Date
- Prior Living Situation

All participating agencies, regardless of funding, must collect, verify, and enter these UDEs into the HMIS within the timeframe outlined in the HMIS Data Quality Plan (Appendix C)
In addition to the universal data elements, there are common program specific data elements. These elements are collected across most Federal Partner programs. Users must also collect all the program-specific data elements at project entry, annual, and exit set forth in the FY 2024 HMIS Data Standards. They are as follows:

- Income and Sources
- Non-Cash Benefits
- Health Insurance
- Physical Disability
- Developmental Disability
- Chronic Health Condition
- HIV/AIDS
- Mental Health Problem
- Substance Use
- Domestic Violence
- Current Living Situation
- Date of Engagement
- Bed-Night Date
- Coordinated Entry Assessment
- Coordinated Entry Event

D. Protecting Privacy Information

The HMIS Staff and HUD are committed to protecting the privacy of clients' information stored electronically or in paper form under the Privacy Act of 1974, as amended, and other federal privacy-related laws, guidance, and best practices. The HMIS Staff and HUD expect all Participating Agencies and Partners who collect, use, maintain, or disseminate clients' information to protect the privacy of that information. Thus, a comprehensive plan for protecting Personally Identifiable Information (PII) has been established and outlined in the document's Security Policies and Procedure section (Item IV).

For more details on the specific requirements of each federal partner, see the referenced program manual.

Manual Name	Federal Partner	Program(s)
CoC Program HMIS Manual - 2024	U.S. Department of Housing and Urban Development (HUD) – Office of Special Needs Assistance Programs (SNAP)	All Continuum of Care (CoC) program component projects
ESG Program HMIS Manual	U.S. Department of Housing and Urban Development (HUD) – Office of Special Needs Assistance Programs (SNAP)	All Emergency Solution Grant (ESG) program component projects
HOPWA Program HMIS Manual	U.S. Department of Housing and Urban Development (HUD) – Office of HIV/AIDS Housing	All Housing Opportunities for Persons with AIDS (HOPWA) program component projects
PATH Program HMIS Manual	U.S. Department of Health and Human Services – Substance Abuse and Mental Health Services Administration	All Projects for Assistance in Transition from Homelessness (PATH) component projects
RHY Program HMIS Manual	U.S. Department of Health and Human Services – Administration for Children and Family Services – Family and Youth Services Bureau	All Runaway and Homeless Youth (RHY) component projects
VA Programs HMIS Manual	Department of Veteran Affairs	SSVF, GPD, and HCHV veteran homeless projects
HUD-VASH Program HMIS Manual	U.S. Department of Housing and Urban Development (HUD) – VASH and Department of Veteran Affairs	Veterans Affairs Supportive Housing (VASH) projects
YHDP Program HMIS Manual - 2024	U.S. Department of Housing and Urban Development (HUD) – Office of Special Needs Assistance Programs (SNAP)	All YHDP component projects

E. HMIS Data Standards Terms and Concepts

1. Continuum of Care and Continuum means the group organized to carry out the responsibilities required under the CoC Program Interim Rule (24 CFR Part 578) and comprises representatives of organizations, including nonprofit homeless providers, victim service providers, faith-based organizations, governments, businesses, advocates, public housing agencies, school districts, social service providers, mental health agencies, hospitals, universities, affordable housing developers, and law enforcement, and organizations that serve homeless and formerly homeless persons to the extent that these groups are represented within the geographic area and are available to participate.
2. CoC Program refers to the HUD funding source which provides housing and/or service grant dollars.
3. Continuum project refers to a distinct unit of an organization, which may or may not be funded by HUD or the Federal Partners, whose primary purpose is to provide services and/or lodging for the homeless and is identified by the Continuum as part of its service system. For example, a project funded by the HUD's CoC Program may be referred to then as a "CoC Program-funded continuum project."
4. HMIS User means the individual who uses or enters data in an HMIS or a comparable database approved by the CoC.
5. HMIS Lead means the entity designated by the Continuum of Care in accordance with the HMIS Proposed Rule (24 CFR Part 580) to operate the Continuum's HMIS on the Continuum's behalf. The Coalition for the Homeless serves as the HMIS Lead

6. HMIS System Administrator means the individual(s) whose job it is to manage the HMIS implementation at the local level: enrolling programs and managing appropriate use, supporting users through connection to, or direct provision of, user training, and overseeing system setup.
7. Project and Program are terms used to mean different things across the federal agencies. In this document, and for the purposes of data collection in HMIS, a program refers to the federal funding source (e.g., HUD CoC, HHS PATH, VA SSVF, YHDP, etc.) whereas project refers to a distinct unit of an organization as set up in the HMIS.

F. HMIS Project Start and Exit Date

End users of any Participating Agency must record the Program Entry Date of a client into HMIS no later than the following for each program type:

1. Emergency Shelters: One (1) workday (24 work hours after the check-in/check-out time)
2. Safe Haven: One (1) workday (24 work hours after the check-in/check-out time)
3. Transitional and Permanent Supportive Housing Programs: Three (3) workdays
4. Rapid Re-Housing and Homelessness Prevention Programs: Three (3) workdays
5. Outreach Programs: Three (3) workdays
6. Supportive Services Only and Other Programs: Three (3) workdays
7. Coordinated Entry: Real-time

End Users of any Participating Agency must record the Project Exit Date of a client into HMIS no later than three (3) business days after exiting the program or receiving their last service. Enabling the "auto-exit" feature is used at the discretion of the HMIS Lead Agency. If enabled, clients enrolled in the program will automatically exit after the defined number of days of not receiving services defined as a "participating service" for that program and record the date of the client's last day in the program as the last day a service was provided.

1. End user must enter the month, day, and year of project enrollment and project exit.
2. For returning clients, end user must record a new Project Entry Date and corresponding Project Exit Date.
3. The system will trigger a warning when end users enter a Project Exit Date that is earlier than the Project Entry Date for a client.

G. HMIS Support Protocol

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

1. HMIS Users should first seek technical support from their agency HMIS expert.
2. If more expertise is required to further troubleshoot the issue, agency HMIS expert or HMIS User should submit request to:
    - IssueTrak at https://hmissupport.homelesshouston.org for all issues related to ClientTrack, or
    - HMIS Support for general technical support at hmis@cfthhouston.org. Refrain from sending email correspondence directly to the HMIS Support Team.
3. HMIS Help Desk line (832-531-6023 or 832-531-6030) is available for HMIS users Tuesday – Thursday (excluding holidays) from 9:00 AM to 11:00 AM and 1:00 PM to 2:00 PM. You must allow until the close of business for a response when you leave a message.
4. Provide issue replication details if possible (or help recreate the problem by providing all information, screenshots, reports, etc.) so HMIS staff can recreate problem if required.
5. The HMIS staff will try to respond to all email inquiries and issues within three (3) business days, but support load, holidays, and other events may affect response time.
6. The HMIS staff will submit a ticket to the software vendor if progress is stalled.

H. HMIS Fees

The TX-700 CoC does not charge a fee for HMIS participation. However, the CoC reserves the right to change this policy should future needs require it. Specialized reports and/or customizations may incur additional fees.

IV. SECURITY POLICIES AND PROCEDURES

A. Protecting Personally Identifiable Information (PII)

Personally Identifiable Information (PII) is defined as information that can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as the date and place of birth, mother's maiden name.

Sensitive Personally Identifiable Information (SPII) is PII that when lost, compromised or disclosed could substantially harm a client. Examples of sensitive PII include social security or driver's license numbers, medical records, and financial account numbers (credit or debit card numbers).

End users and all Participating Agencies are required to take the necessary steps to help ensure compliance with the Privacy Act and other privacy-related laws.

a. Manage and Limit Access to Sensitive PII
   1. Only share or discuss sensitive PII with those who have a need to know for work purposes.
   2. Do not distribute or release sensitive PII to others until the release is authorized.
   3. Before discussing sensitive PII on the telephone, confirm that you are speaking to the right person and inform them that the discussion will include sensitive PII.
   4. Do not leave messages containing sensitive PII on voicemail.
   5. Avoid discussing sensitive PII if unauthorized persons are in the adjacent cubicles, rooms, or hallways and may overhear your conversations.
   6. If sensitive PII will be discussed, hold meetings in secure spaces (no unauthorized access or eavesdropping possible).
   7. Treat notes and minutes from such meetings as confidential unless you can verify that they do not contain sensitive PII. Record the date, time, place, subject, chairperson, and attendees at any meeting involving sensitive PII.

b. Protect Hard Copy and Electronic Files Containing Sensitive PII
   1. Lock up all hard copy files containing sensitive PII in secured file cabinets.
   2. Do not leave sensitive PII unattended in an open area.
   3. Protect all media (e.g., flash drives) that contain sensitive PII and do not leave them unattended. This information should be maintained either in secured file cabinets or in secured computers.
   4. Keep accurate records of where PII is stored, used, and maintained.
   5. Secure digital copies of files containing PII. Protections include encryption, implementing enhanced authentication mechanisms such as two-factor authentication, and limiting the number of people allowed access to the files.
   6. Store sensitive PII only on workstations that can be secured, such as workstations located in areas that have restricted physical access.

c. Protecting Electronic Transmissions of Sensitive PII email, etc.
   1. When sending sensitive PII via email or via an unsecured information system, make sure the information and any attachments are encrypted.
   2. For each event, the best course of action is to limit access to PII only to those authorized to handle it, create a paper trail, and verify that the information reached its destination.
   3. Do not place PII on shared drives, multi-access calendars, the Intranet, or the Internet.
   4. Do not let PII documents sit on a printer where unauthorized employees or contractors can have access to the information.

d. Protecting Hard Copy Files Containing Sensitive PII
   1. Do not remove records with sensitive PII from facilities where the information is authorized to be stored or accessed remotely unless approval is first obtained from a supervisor.
   2. Do not use interoffice or translucent envelopes to mail sensitive PII. Use sealable opaque solid envelopes. Mark the envelope to the person's attention.

3. When using the U.S. postal service to deliver information with sensitive PII, double-wrap the document (use two envelopes – one inside the other) and mark only the inside envelope as confidential with the statement – To Be Opened by Addressee Only.
4. If PII needs to be sent by courier, mark "signature required" when sending documents in order to create a paper trail in the event items are misplaced or lost.

e. Records Management, Retention and Disposition
1. Follow all applicable records management laws, regulations, and policies.
2. Do not maintain records longer than required.
3. Destroy records after retention requirements are met.
4. Dispose of sensitive PII appropriately and permanently erase electronic records. Also, shred hard copy records.

Incident Report. A data breach occurs when PII is viewed, leaked, or accessed by anyone other than the individual or someone authorized to have access to this information as part of their official duties. Compromises of sensitive PII related to HMIS programs should be reported to the HMIS Lead Agency by emailing hmis@cfthhouston.org. Upon receiving the report, the Lead Agency will investigate the issue and inform the Partner Agency about the next steps.

B. Training

Each end user must complete the required New User Training prior to gaining access to HMIS. HMIS staff will provide training to all end users

A. HMIS staff will provide New User Training to proposed end users.
B. HMIS staff will provide new end users with a copy of the HMIS Policies and Procedures and HMIS User Guide.
C. The table below lists the training courses offered.

Course Description	Course Detail
New User Training	Users will learn the basic skills and concepts needed in order to complete the client intake process.
Refresher Training	Help to refresh the skills of active users, as well as review any issues users may have with navigating through the system or the data collection process.
Reports Training	Users are given an overview of the various reporting options available in ClientTrack.
Data Explorer	Trains experienced users, with good knowledge of existing ClientTrack reports, on the usage of ClientTrack's ad hoc data analysis tool. (Limited to one user per agency per session)
Advanced or Specialized Training	Focuses on specific areas of need, including the use of new technologies or apps, such as Eva Analytics.

Additionally, each end user must complete annual security training provided by HMIS Staff. Failure to complete this training will result in user account suspension until the training has been completed. Refresher training is required of all new users three months after initial training. Accounts will be deactivated if the refresher is not attended.

C. User Authentication

Only users with a valid username and password combination can access HMIS. The HMIS staff will provide unique username and initial password for eligible individuals after completion of required training and signing of the HMIS User License Agreement.

1. The Participating Agency will determine which of their employees will have access to the HMIS. User access will be granted only to those individuals whose job functions require legitimate access to the system.
2. Proposed end user must complete the required training and demonstrate proficiency in use of system.
3. Proposed end user must sign the HMIS User License Agreement stating that he or she has received training, will abide by the Policies and Procedures, will appropriately maintain the confidentiality of client data, and will only collect, enter and retrieve data in the system relevant to the delivery of services to people.
4. The HMIS staff will be responsible for the distribution, collection, and storage of the signed HMIS User License Agreements.
5. The HMIS staff will assign new users with a username and an initial password.
6. Sharing of usernames and passwords is a breach of the HMIS User License Agreement since it compromises the security to clients. Violation will result in loss of username of all parties and a consult session with manager/director/ED.
7. The Participating Agency is required to notify the HMIS staff when end user leaves employment with the agency or no longer needs access.
8. Users not logging into HMIS for more than 45 days will be locked out due to non-activity.

D. Passwords

Each end user will have access to HMIS via a username and password, which will be reset every 365 days.

1. The HMIS staff will provide new end users with a unique username and temporary password after completing the initial training.
2. The end user will be required to create a permanent password between eight and sixteen characters in length. It must also contain characters from the following four categories: (1) uppercase characters (A through Z), (2) lowercase characters (a through z), (3) numbers (0 through 9), and (4) non-alphabetic characters (for example, $, #, %).
3. The end user will securely maintain their password and never share it with others.
4. Access permission will be revoked after the end user unsuccessfully attempts to log on five times.
5. As an additional security measure, the end users can set up a 2-step verification process.

E. Hardware Security Measures

All computers and networks used to access HMIS must have virus protection software and firewall installed. Virus definitions and firewall must be regularly updated.

F. Security Violations and Sanctions

Any end user found to be in violation of security protocols of their agency's procedures or HMIS Policies and Procedures will be sanctioned accordingly. All end users must report potential violations of any security protocols.

1. End users are obligated to report suspected instances of noncompliance and/or security violations to their agency and/or HMIS staff as soon as possible.
2. The Participating Agency or HMIS staff will investigate potential violations.
3. Any end user found to be in violation of security protocols will be sanctioned accordingly. Sanctions may include but are not limited to suspension of system privileges and revocation of system privileges.

G. Equal Access

All end users and participating agencies must adhere to an environment that embraces diversity, respects the rights of all individuals, is open and accessible, and is free of harassment and discrimination based on, but not limited to, ethnicity, race, creed, color, religion, age, disability, sex, marital status, national origin, genetic information, political opinions or affiliations, and veteran status in all its programs, activities, and employment.

V. DATA POLICIES AND PROCEDURES

A. Data Quality

Data quality refers to the timeliness, completeness, and accuracy of information collected and reported in the HMIS. All data entered into the HMIS must meet data quality standards. Participating agencies will be responsible for their users' data quality.

1. Data Timeliness:

   End users must enter all universal data elements and program-specific data elements using the guidelines identified in the HMIS Data Quality Plan (Appendix C).

2. Data Completeness:

   All data entered into the system is complete.

3. Data Accuracy:

   All data entered shall be collected and entered in a common and consistent manner across all programs.

   a. Participating Agencies must sign the HMIS Agency Participation Agreement (Appendix A) to ensure that all participating programs are aware of and have agreed to the data quality standards.

b. Upon agreement, Participating Agencies will collect and enter as much relevant client data as possible for the purposes of providing services to that client.
c. The HMIS staff will conduct monthly checks for data quality. Any patterns of error or missing data will be reported to the Participating Agency.
d. End users will be required to correct the identified data error and will be monitored for compliance by the Participating Agency and the HMIS staff.
e. End users may be required to attend additional training as needed.

B. Preventing Client Duplication at Program Entry

The most important method for reducing duplication in the HMIS is effectively using the search criteria before adding client-level data. Users must search the database to determine whether the client has already been entered into the HMIS before adding a new record.

Limiting the search to just the last name field is the most effective way to search for clients in the database. Searching for a client using multiple fields or full demographics increases the likelihood of duplication because the client might have been entered with slightly different information. Different search methods can be used by combining partial first name, partial last name, alias, birth date, or social security number (SSN). Using wildcard characters (*) may help with the search.

It is recommended that the SSN or alias fields be used with great care. Searching by just the SSN increases the likelihood of error due to transposition errors. The HMIS contains many client records, and every search for a client should be conducted as if the client's record already exists. If all the recommended search strategies have been exhausted, then a new client record should be created.

C. Data Use and Disclosure

All end users will follow the data use Policies and Procedures to guide the data use of client information stored in HMIS.

Client data may be used or disclosed for system administration, technical support, program compliance, analytical use, and other purposes as required by law. Uses involve sharing parts of client information with persons within an agency. Disclosures involve sharing parts of client information with persons or organizations outside an agency.

Participating Agencies may use data in the system to support the delivery of services to homeless clients in the CoC. Agencies may use or disclose client information internally for administrative functions, technical support, and management purposes. Participating Agencies may also use client information for internal analysis, such as analyzing client outcomes to evaluate the program.

The software vendor and any authorized subcontractor shall not disclose data stored in HMIS without expressed written permission by the HMIS Lead Agency. A service agreement, signed by the HMIS Lead Agency and the vendor, will contain language that prohibits access to the data except under the conditions specified in the agreement.

D. Data Release

All HMIS stakeholders will follow the data release Policies and Procedures to guide the data release of client information stored in HMIS.

Data release refers to the dissemination of aggregate or anonymous client-level data for the purposes of system administration, technical support, program compliance, and analytical use.

1. No identifiable client data will be released to any person, agency, or organization for any purpose without written permission from the client, unless covered by Privacy Policy release exceptions such as court orders and related requests.
2. Aggregate data may be released without agency permission at the discretion of the Continuum. It may not release any personal identifiable client data to any group or individual.

E. Custodian of Records to Legal Requests for HMIS Data

The CFTH HMIS Lead and Administration reserves the right to respond to legal requests, court orders, or proceedings as required by law. Thus, the Director of HMIS Administration is the authorized staff responsible for ensuring proper execution of such subpoenas to help maintain compliance with applicable security, confidentiality, and consent protocols. The HMIS External Partner Engagement Manager will be the proxy. The procedure for responding to subpoenas and/or other related requests is outlined below.

1. **Receipt:** Any staff receiving a subpoena or related request must immediately forward it to the Director of HMIS Administration, Custodian of Records.
2. **Review:** The Director of HMIS Administration will notify the Director of Public Affairs (or "legal counsel for CFTH") of the request. The Director of HMIS Administration and the Director of Public Affairs (or "legal counsel for CFTH") will review the request to determine the validity and scope; whether client consent is required; and whether the record can or must be withheld due to legal protections.
3. **Response:** If the request is valid and permissible, the Director of HMIS Administration will compile the relevant HMIS data. The Director of HMIS Administration and the Director of Public Affairs (or "legal counsel for CFTH") will review the data and release it, adhering to applicable laws. The response will be documented, including what was disclosed, to whom, and under what authority.

VI. CLIENT CONSENT, PRIVACY AND RIGHTS

A. Client Consent

Participating Agencies must obtain informed, consent prior to entering any clients personal identifiable information into HMIS. Services will not be denied if a client chooses not to include personal information. Personal information collected about the client should be protected. Each Participating Agency and end user must abide by the terms in the HMIS Agency Participation Agreement (Appendix A) and HMIS User License Agreement (Appendix B).

1. Client must provide consent, verbal or written. The HMIS Client Consent and Release form (Appendix D) should be used for written consent.
2. Clients that provide permission to enter personal information allow for Participating Agencies within the continuum to share client and household data.

3. If client refuses consent, the end user should not include any personal identifiers (First Name, Last Name, Social Security Number, and Date of Birth) in the client record.
4. For clients with consent refused, end user should include a client identifier to recognize the record in the system.
5. Participating Agencies shall uphold Federal and State Confidentiality regulations and laws that protect client records.

B. Client Privacy

The HMIS standards and the HIPAA standards are mutually exclusive. An organization that is covered under the HIPAA standards is not required to comply with the HMIS privacy or security standards, so long as the organization determines that a substantial portion of its protected information about homeless clients or homeless individuals is indeed protected health information as defined in the HIPAA rules.

HIPAA standards take precedence over HMIS because HIPAA standards are finely attuned to the requirements of the health care system; they provide important privacy and security protections for protected health information; and it would be an unreasonable burden for providers to comply with and/or reconcile both the HIPAA and HMIS rules. This spares organizations from having to deal with the conflicts between the two sets of rules.

Victim services providers that are recipients or subrecipients under the CoC Program and covered under the Violence Against Women Act (VAWA) are required to collect client-level data consistent with HMIS data collection requirements, BUT they must not directly enter data into an HMIS. To protect clients, victim services providers must enter required client-level data into a comparable database that complies with HMIS requirements. They may use CoC Program funds to establish and operate a comparable database. Information entered into a comparable database must not be entered directly into or provided to an HMIS. Victim services providers MUST provide aggregate data to the CoC for reporting purposes.

C. Client Grievance

It is the policy of the Coalition to ensure that clients serviced by this organization and its partner agencies have the right to respectful and responsive services. We are committed to providing a clear grievance process for those served in our programs and their authorized or legal representatives to bring grievances forward and have them resolved in a timely manner.

All participants have the right to file formal grievances if they feel they are not being treated fairly, have problems with the behaviors of others (either staff or other participants), or disagree with program components. If there is a problem, it is requested that you sincerely try to resolve the issue with the person or persons involved.

If there is a grievance regarding Coalition for the Homeless Case Management staff and efforts to resolve it directly have not been successful, it is recommended to follow The Way Home COC-Grievance Policy to file a complaint (See Appendix H for TX-700 The Way Home COC-Grievance Policy).

Grievances regarding organizations other than the Coalition for the Homeless will be forwarded to that organization (See Appendix G for HMIS Client Grievance Policy). Coalition staff and other outreach, shelter, and housing organization staff work closely to prevent confusion and misunderstandings regarding rules, policies, expectations, and procedures.

If a participant feels mistreated by another participant in the program, they are encouraged to confront the peer in a healthy manner. The participant may request staff assistance in resolving the issue. This process is in place to assist participants in developing confrontation tools.

Contacts

VP of Program Operations
James Gonzalez
Jgonzalez@cfthhouston.org

VP of Homeless Response System (HRS)
Renee Cavazos
rcavazos@cfthhouston.org

Mail to: Coalition for the Homeless Houston/Harris County 2000 Crawford, Suite 700
Houston Tx 77002

VII. APPENDICES

Appendix	Document Title
Appendix A	HMIS Agency Participation Agreement
Appendix B	HMIS User License Agreement
Appendix C	HMIS Data Quality Plan
Appendix D	HMIS Client Consent and Release
Appendix E	HMIS Privacy Policy
Appendix F	HMIS Fee Schedule
Appendix G	HMIS Client Grievance Policy