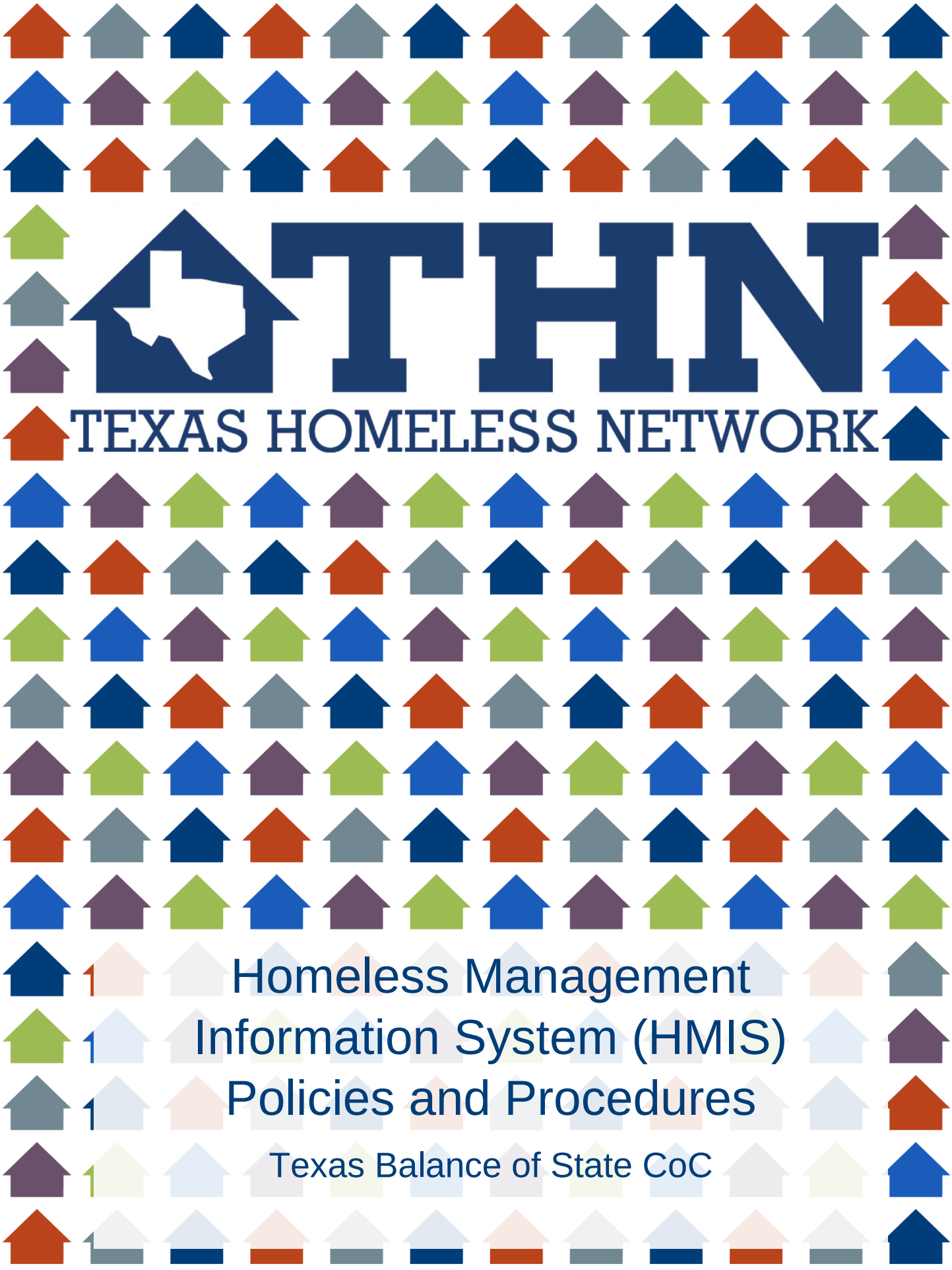

Homeless Management Information System (HMIS) Policies and Procedures

Texas Balance of State CoC

Table of Contents

Project Summary 4
Introduction 4
History 4
Why is this important? 4
Roles and Responsibilities 5
CoC and CoC Board Responsibilities 5
Data Committee Responsibilities 5
Texas Balance of State CoC HMIS Lead Responsibilities 5
Covered Homeless Organization (CHO) Responsibilities 6
Implementation Policies and Procedures 6
HMIS End User Access 6
HMIS New Agency Application 7
HMIS User Agreement 7
HMIS Administrator Agreement 7
Data Collection Requirements 8
HMIS Program Entry and Exit Date 9
HMIS Technical Support Protocol 9
Participation Fees 10
Security Policies and Procedures 10
Regarding HMIS Users Currently Experiencing Homelessness 10
Victim Service Providers, Survivors, and HMIS 10
Training 11
User Authentication 12
Passwords 13
Hardware Security Measures 13
Data Disposal 13
Security Review 13
Security Violations and Sanctions 13
Security Violations and Sanctions for Law Enforcement 14
Whistleblower/Complaint Policy 14
Client Informed Consent and Privacy Rights 15
Uses and Disclosures without Client Consent 15
Uses and Disclosures with Client Consent 16

Client Consent Refusal Procedures 18
Data Policies and Procedures 19
Data Retrieval and Sharing 19
Data Quality 19
Data Timeliness 19
Data Completeness 20
Data Accuracy 20
Data Reporting and Performance Management 20
Data Use and Disclosure 21
Data Release 22
Resources 22

Project Summary

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.

Texas Balance of State HMIS is staffed at Texas Homeless Network (THN). THN has been designated by the Continuum of Care (CoC) as the HMIS Lead Agency to operate the HMIS to ensure high data quality and other HUD HMIS compliance of all HUD CoC and ESG Program Projects and other projects required to use HMIS in the Texas Balance of State CoC. The HMIS Lead Agency also ensures the same standards and protocols for non-funded participating agencies. THN performs these tasks at the direction of the CoC, through the TX BoS CoC Board.

Agencies that participate in Texas Balance of State's HMIS are referred to as Covered Homeless Organizations (CHO). Each CHO 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.

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 Continuums 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.

Why is this important?

Having access to the HMIS represents a strategic advantage for service providers. The HMIS software selected by the Texas Balance of State CoC 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.

Roles and Responsibilities

CoC and CoC Board Responsibilities

- Select and designate an HMIS Software for the CoC.
- Select and designate an HMIS Lead for the CoC, among eligible applicants.
- Review and approve *HMIS Policies and Procedures*.
- Review and approve the *Data Quality Plan*.
- Work with the HMIS Lead to ensure consistent agency participation across the CoC.
- Evaluate performance of the HMIS Software and HMIS Lead.

Data Committee Responsibilities

This committee will be responsible for the following:

- In partnership with the CoC Lead and HMIS Lead: developing, following, and updating annually an HMIS Governance Charter, which will include all procedures and policies needed to comply with 24 CFR 578.7(b), its subparts, and the HMIS requirements, as prescribed by HUD;
- Developing, annually reviewing, and, as necessary, revising for Board approval, a privacy plan, security plan, and data quality plan for the HMIS;
- Assessing and reporting to the Board regarding participation in HMIS by users throughout the CoC geography;
- Developing for Board approval and implementing a plan for monitoring the HMIS to ensure that:
    - Recipients and subrecipients consistently participate in HMIS;
    - HMIS is satisfying the requirements of all regulations and notices issued by HUD; and
    - The HMIS Lead is fulfilling the obligations outlined in its HMIS Governance Charter, including the obligation to enter into written participation agreements with each contributing HMIS organization (CHO); and
    - Overseeing and monitoring HMIS data collection and production of the following reports:
        - Sheltered Point-in-Time (PIT) Count;
        - Housing Inventory Count (HIC);
        - Longitudinal System Analysis (LSA);
        - Annual Performance Reports (APRs); and
        - System Performance Measures (SPMs).

Texas Balance of State CoC HMIS Lead Responsibilities

- Execute HMIS participation agreements;
- Monitor CHOs compliance with applicable HMIS standards on a regular basis;
- Establish and review annually End User Agreements;
- Maintain and update as needed the files for HMIS software to include software agreements, HUD Technical Submissions, HUD executed agreements and Annual Performance Reports;

- 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;
- Develop and update as needed a Data Quality Plan;
- Review and update HMIS Privacy Policy yearly;
- Develop and review annually the HMIS Security Plan, including disaster planning and recovery strategy;
- Review and update as need HMIS Policies and Procedures;
- Provide copies of the Data Quality Plan, Privacy Policy, Security Plan and Policy and Procedures to the Data Committee for review and feedback on an annual basis;
- Review national, state and local laws that govern privacy or confidential protections and make determinations regarding relevancy to existing HMIS policy;
- Provide new user training and refresher user training monthly (except for the month of December due to billing matters);
- Pro-actively contact new users for immediate follow up and issuance of username and password to access HMIS in an effort to begin entry of data as soon as possible following training;
- Provide on-site technical support to agencies using HMIS for trouble-shooting and data input;
- Quarterly review of HMIS data and bed lists to ensure that CHO programs are using HMIS accurately;
- Provide assistance to agencies upon request for additional on-site training and support
- Conduct unduplicated accounting of homelessness annually.

Covered Homeless Organization (CHO) Responsibilities

- Must comply with all applicable agreements;
- Conduct background checks on all staff who will have access to HMIS (this will be asked during CHO self-audits). Based on the outcome of the background check, the CHO will determine which individuals should seek HMIS access;
- Execute and manage HMIS User Agreements with all staff who have HMIS access;
- Comply with the HMIS Standards as appropriate;
- Accurately enter all required data into the HMIS system, including accurate and timely information into housing, where applicable;
- Display the Privacy Notice in intake areas (this will be asked during CHO self-audits);
- Provide a copy of the Privacy Policy upon client request (this will be asked during CHO self-audits)
- Complete annual self-audit to be returned to Texas Balance of State CoC HMIS Lead Agency.

Implementation Policies and Procedures

HMIS End User Access

The TX BoS CoC understands that in order to make homelessness rare, brief, and nonrecurring, multiple stakeholders need to be involved in HMIS participation. Potential CHOs

may include non-profit organizations, local governments, healthcare systems, and law enforcement.

In regards to law enforcement, the TX BoS CoC limits HMIS access only to the homeless outreach team members associated with a specific police department. This decision was made by the TX BoS CoC Data Committee on August, 31st, 2021, and is subject to change.

At this time, the Data Committee recommends the following conditional access for law enforcement: homeless outreach team members will have write, view, and edit access for Street Outreach programs, and for Coordinated Entry purposes, they will have view access and the ability to make referrals.

Furthermore, the TX BoS CoC HMIS Lead requires that each end-user completes their own HMIS user agreement. Therefore, it is essential that end-users must be at least 18 years of age in order to meet all end-user requirements.

HMIS New Agency Application

The Executive Director of any CHO shall follow, comply, and enforce the HMIS New Agency Application. The Executive Director must sign an HMIS New Agency Application before granted access to HMIS. Signing of the HMIS New Agency Application is a precursor to training and user access.

- Approval of the HMIS New Agency Application is at the discretion of the TX BoS CoC HMIS Lead.
- An original signed HMIS New Agency Application must be presented to the HMIS staff before any program is implemented in the HMIS.
- After the HMIS New Agency Application is signed, the HMIS staff will train end users to use HMIS.
- A username and password will be granted to end users after required training is completed.

HMIS User Agreement

An HMIS end user of any CHO shall follow, comply, and enforce the HMIS User Agreement. Before given access to HMIS, the end user must sign an HMIS User Agreement.

- HMIS end users will need to re-sign their HMIS User Agreement annually; this annual re-sign will happen after the annual HMIS Data Security and Ethics Training
- The HMIS staff will provide the end user a HMIS User Agreement for signature after completing required training.
- The HMIS staff will collect and maintain HMIS User Agreements of all end users.

HMIS Administrator Agreement

An HMIS Administrator of any CHO shall follow, comply, and enforce the HMIS Administrator Agreement. Each CHO must designate a local HMIS Administrator. This person must be a current HMIS end user and knowledgeable of all day-to-day case management operations and procedures.

- HMIS Administrators are the primary contact for all communication regarding the HMIS at their agency.

- HMIS Administrators provide a point-of-communication between the HMIS end users and THN.
- HMIS Administrators provide HMIS end users with up-to-date information about the system and general technical assistance
- HMIS Administrators assist with purchasing and managing HMIS licenses
- HMIS Administrators will need to re-sign their HMIS Administrator Agreement annually; this annual re-sign will happen after the annual HMIS Administrator Training
- The HMIS staff will provide the HMIS Administrator with an HMIS Administrator Agreement for signature after completing required training.
- The HMIS staff will collect and maintain HMIS Administrator Agreements of all administrators.

Data Collection Requirements

CHOs will collect and verify the minimum set of data elements for all clients served by their programs within the timeframe outlined in the HMIS Data Quality Plan.

During client intake, end users must collect all the Universal Data Elements (UDEs) set forth in the most recent version of the HMIS Data Standards Manual, May 2021. The Universal Data Elements include:

- Name
- Social Security Number
- Date of Birth
- Race
- Ethnicity
- Gender
- 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

End users must also collect all the program-specific data elements at program entry and exit set for in the most recent version of the HMIS Data Standards Manual. The program-specific data elements include:

- Income and Sources
- Non-Cash Benefits
- Health Insurance
- Physical Disability
- Developmental Disability
- Chronic Health Condition
- HIV/AIDS

- Mental Health Disorder
- Substance Use Disorder
- Domestic Violence
- Current Living Situation
- Date of Engagement
- Bed-Night Date
- Coordinated Entry Assessment
- Coordinated Entry Event

HMIS Program Entry and Exit Date

End users of any CHO must record the data into HMIS within the following days:

Project	Timeframe
Emergency Shelter	• Universal data elements and housing check-in/check-out are entered within **1 business day** & • Assessment entered within **1 business day** of enrollment.
Homeless Prevention & Rapid Re-Housing	Universal Data Elements/Assessments are entered within **1 business day** of enrollment.
Transitional and Permanent Supportive Housing	Universal Data Elements and Housing Check-in/Check-Out entered within **3 business days** of enrollment.
Outreach	• Personally identifiable information (PII) entered within **3 business days** of initial engagement & • Universal Data Elements/Assessment entered within **3 business days** of enrollment.
Supportive Services Only	Universal Data Elements/Assessments entered within **3 business days** of enrollment.

Enabling the “auto-exit” feature for programs is available at the CHO’s discretion. 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.

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

HMIS Technical Support Protocol

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

HMIS Users should first seek technical support from their agency HMIS expert. If more expertise is required to further troubleshoot the issue, agency HMIS expert or HMIS User should submit request to HMIS Support for general technical support at hmis@thn.org.

Technical Support Hours are Monday through Friday (excluding holidays) from 9:00 AM to 5:00 PM.

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.

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.

The HMIS staff will submit a ticket to software vendor if progress is stalled.

Participation Fees

The Texas Balance of State CoC reserves the right to charge a license fee to use the system.

Each annual user license subscription is active for a full calendar year. If user licenses are purchased after the start of the new year, they will be prorated. HMIS license fees are prorated based on when an agency begins using HMIS. For example, if an agency begins using the system in July, the HMIS invoice is prorated for six (6) months for a total of $175 per user. Currently the annual license pricing is, one (1) HMIS license is $350 and five (5) HMIS licenses are $1400 and (1) read-only access license is $100. The read-only access license differs from a normal HMIS license. Users with the read-only license can access files and reporting but the permissions are set so the user is only allowed to read and not make changes.

Security Policies and Procedures

Regarding HMIS Users Currently Experiencing Homelessness

Some CHOs may want to purchase HMIS licenses for users who are either currently experiencing homelessness or who are formerly homeless. This may raise questions on both the CHO and community-level about privacy and security in regards to users who may currently have their own records in HMIS or may personally know others with records in HMIS.

HUD has not released specific guidance addressing current and/or former clients' access to HMIS. However, Section 4.2.6 of the 2004 HMIS Technical Standards applies to anyone from a covered homeless organization (CHO) that is accessing HMIS: "... A CHO must require each member of its staff (including employees, volunteers, affiliates, contractors and associates) to sign (annually or otherwise) a confidentiality agreement that acknowledges receipt of a copy of the privacy notice and that pledges to comply with the privacy notice." This requirement ensures that all users of the system agree to comply to the same set of standards and the same set of consequences if the agreement is broken.

TX BoS CoC requires that all CHOs give the same resources in regards to HMIS training and re-training protocols to those HMIS users currently experiencing homelessness as those HMIS users who are not experiencing homelessness.

Victim Service Providers, Survivors, and HMIS

Victim Service Providers are statutorily prohibited from entering information into HMIS. However, for the purposes of Coordinated Entry a workaround was created by the TX BoS CoC

and the Texas Council on Family Violence (TCFV) to allow for Victim Service Providers to be Entry Points and for households to be entered into HMIS while remaining safe and secure. Coordinated Entry regions must follow this workaround for survivors who are served by Victim Service Provider Entry Points. Please review the Texas Balance of State Continuum of Care Coordinated Entry Written Standards for more information on the appropriate protocols for the Victim Service Workaround.

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
- HMIS staff will provide New User Training to proposed end users.
- HMIS staff will provide new end users with a copy of the HMIS Policies and Procedures and the HMIS Privacy Policy

Potential end users will need to request HMIS training using a form found on our website. ***(This is not the form used to request Coordinated Entry Training.)*** Training consists of two distinct parts: an online video portion and a hands-on exercise.

New end users are required to complete at least three online courses: A course that covers their specific project type as indicated on their training request, a data security course, and an HMIS assessments course. Each course has a set of quizzes at the end of each video to check for understanding. Users may be assigned more than these three courses if they request multiple projects or funding types whose intakes are significantly different from each other.

Once those courses are completed, end users will receive a training task list along with login information for our training version of HMIS. The task list will ask the end user to create enrollments, services, case notes, referrals, etc. The HMIS Training Coordinator will then review the end user's work in the training site. The end user will be considered done with training after all online courses and the task list are completed.

End users needing Coordinated Entry HMIS training will need to submit a different form found in the Texas Balance of State CoC Coordinated Entry Google Drive. End users from CE Entry Points will have two online courses covering the foundations of CE and what CE looks like in HMIS. End users must also complete a task list similar to the ones used during New User Trainings. For those users who utilize HMIS for CE purposes only, the following trainings will be assigned: two online courses covering the foundations of CE and what CE looks like in HMIS and Data Security/Ethics training.

The table below lists the training courses offered.

Course	Course Description
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.
Coordinated Entry Training	Specific to agencies participating in their communities Coordinated Entry System. Users will learn how to complete a CE intake and the CE referral process.
Data Security/Ethics Training	A mandatory, annual training focusing on HMIS security and ethics. New users also go through this training as part of their new user course.
Assessments Training	Specifically covers the four main types of assessments in HMIS: Entry, Exit, Annual, and During Program Enrollment. End users learn how these assessments are created and when they should be created.

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 Agreement.

- The CHO 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.
- Proposed end user must complete the required training and demonstrate proficiency in use of system.
- Proposed end user must sign the HMIS User Agreement stating that the user 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.
- The HMIS staff will be responsible for the distribution, collection, and storage of the signed HMIS User Agreements.
- The HMIS staff will assign new users with a username and an initial password.
- Sharing of usernames and passwords is a breach of the HMIS User Agreement since it compromises the security to clients.
- The CHO is required to notify the HMIS staff when end user leaves employment with the agency or no longer needs access.
- Users not logging into HMIS for more than 45 days will be locked out due to non-activity.
- Users not logging into HMIS for the time frame of 46-90 days will be required to retake virtual trainings.

- Users not logging into HMIS for 91+ days are required to retake virtual trainings and complete the new user task list.

Passwords

- Each end user will have access to HMIS via a username and password. Passwords will be reset every 180 days. End users will maintain passwords confidential.
- The HMIS staff will provide new end users a unique username and temporary password after required training is completed.
- End user will be required to create a permanent password that is between eight and sixteen characters in length. It must also contain characters from the following four categories: (1) uppercase characters (A through Z), (2) lower case characters (a through z), (3) numbers (0 through 9), and (4) non-alphabetic characters (for example, $, #, %).
- End users may not use the same password consecutively, but may use the same password more than once.
- Access permission will be revoked after the end user unsuccessfully attempts to log on six times. The end user will be unable to gain access until the HMIS Admin or HMIS staff reset their password.

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.

Data Disposal

In order to delete all HMIS data from a data storage medium, a CHO must reformat the storage medium. A CHO should reformat the storage medium more than once before reusing or disposing the medium.

A CHO may commit itself to additional security protections consistent with HMIS requirements by destroying media (re: paper copies of files or computer hardware with digital files) at a bonded vendor to ensure all the HMIS data is completely destroyed.

Security Review

CHOs are required to complete an annual security review, also called a self-audit, to ensure the implementation of the security requirements. The security review will include the completion of a security checklist ensuring that each security standard is implemented. The TX BoS CoC board has selected a member of the Data Team to serve as the Security Officer, who will certify CHO self-audits have been completed.

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. End users found in violation may be temporarily or permanently suspended from HMIS based on an investigation of the violations.

The table below lists the progression of warnings and actions taken by the CoC in cases of security violations. The CoC reserves the right to immediately and permanently revoke access from a user without a full three warnings depending on the severity of the violation(s).

Warnings	Result
First Warning	End User, CHO HMIS Admin, and CHO Executive Director are informed of violation and are put on notice to create plan to ensure violation doesn't happen again.
Second Warning	Temporary suspension from HMIS with mandatory refresher training to ensure end user understands proper HMIS security procedures and expectations.
Third Warning	Permanent suspension from HMIS; this may not be appealed.

Security Violations and Sanctions for Law Enforcement

In regards to law enforcement, if an end-user is found to be in violation of security protocols of their agency's procedures or HMIS Policies and Procedures will be sanctioned accordingly. Per our HMIS User Agreement, the HMIS Lead may terminate a User license for a number of reasons, including fraud, misuse, negligence, license sharing, inactivity, and client duplication.

Warnings	Result
First Warning	Temporary suspension from HMIS with mandatory refresher training to ensure end user understands proper HMIS security procedures and expectations.
Second Warning	Permanent suspension from HMIS; this may not be appealed.

Whistleblower/Complaint Policy

In keeping with the policy of maintaining the highest standards of conduct and ethics, Texas Homeless Network (THN) will investigate complaints of suspected fraudulent or dishonest use or misuse of the Homeless Management Information System (HMIS) by staff, board members, consultants, HMIS end-users, volunteers, Covered Homeless Organizations (CHOs), clients, and community members. To maintain the highest standards of service, THN will also investigate complaints concerning internal and external misconduct of programs and services.

Staff, board members, consultants, HMIS end-users, volunteers, CHOs, clients, and community members must report suspected fraudulent or dishonest conduct or problems with services provided, data sharing, or misuse of HMIS, pursuant to the procedures set forth below. This policy supplements, and does not replace, any procedures required by law, regulation, or funding source requirements.

Reporting Responsibilities: This Whistleblower/Complaint Policy is intended to encourage staff, board members, consultants, HMIS end-users volunteers, CHOs, clients, and community members to raise serious concerns to THN so they can be addressed and appropriate actions can be taken.

Compliance Officer: THN's Director of Data will act as the Compliance Officer and is responsible for ensuring that all complaints about unethical or illegal conduct are investigated

and resolved. The Compliance Officer will advise THN's President/CEO of all complaints and their resolution.

Reporting Procedure: THN has an open-door policy and encourages all staff, board members, consultants, HMIS end-users, volunteers, CHOs, clients, and community members to share their questions, concerns, suggestions, and complaints to the Compliance Officer as well as the leadership of the agency in question. A person's concerns about possible fraudulent or dishonest use or misuse of the HMIS system, data, resources, or program operation, should be reported immediately to the Compliance Officer. If, for any reason, a person finds it difficult to report their concerns to such person, they may report the concerns directly to THN's President/CEO. Alternately, to facilitate reporting of suspected violations where the reporter wishes to remain anonymous, a written statement may be submitted to via the HMIS Whistleblower/Complaint form.

Investigation: All relevant matters, including suspected but unproved matters, will be promptly reviewed and analyzed, with documentation of the receipt, retention, investigation, and treatment of the complaint. Appropriate corrective action will be taken, if necessary, and findings may be communicated to the reporting person and their supervisor, if appropriate. Investigations may be conducted by THN staff as well as independent persons such as auditors and/or attorneys. Investigators will maintain appropriate confidentiality to the extent possible.

No Retaliation: No staff, board members, consultants, HMIS end-users, volunteers, CHOs, clients, and community members who in good faith reports suspected fraudulent or dishonest use or misuse of the HMIS system, data, resources, or program operation that THN oversees shall suffer harassment, retaliation, or adverse consequences. The Policy is in addition to any non-retaliation requirements required by law.

This protection from retaliation is not intended to prohibit THN staff from acting, including disciplinary action based on the policies set forth in the following forms: New Agency Application, Administrator Agreement, and HMIS User Agreement. Individuals making complaints must be cautious to avoid baseless allegations; staff, board members, consultants, HMIS end-users, volunteers, CHOs, clients, and community members who intentionally make false allegations are subject to disciplinary action.

Client Informed Consent and Privacy Rights

Collecting and sharing participants' personal information is often a necessary aspect of helping persons to resolve their housing crisis. The HMIS Lead Agency and CHOs may only collect, use, and disclose data for the specific purposes and reasons defined in this section.

The CHO must display the Privacy Notice in all intake areas where clients can easily see. CHOs must also provide a copy of the Privacy Policy to the client upon request.

Uses and Disclosures without Client Consent

HUD gives CHOs the authority for the following uses and disclosures without needing to obtain participant consent for the reasons below as referenced in the Privacy Notice.

- Providing or coordinating services to an individual
- Creating de-identified records from PPI

- Carrying out administrative functions including but not limited to audit, personnel oversight, and management functions;
- Functions related to payment or reimbursement for services
- To provide or coordinate individual referrals, case management, housing, or other services. Client records may be shared with other organizations that may have separate privacy policies and that may allow different uses and disclosures of the information;
- For functions related to payment or reimbursement for services;
- To produce aggregate-level reports regarding use of services;
- To produce aggregate-level reports for funders or grant applications;
- To create de-identified (anonymous) information;
- To track system-wide and project-level outcomes;
- To identify unfilled service needs and plan for the provision of new services;

Coordinated Entry-related uses and disclosures are as follows:

Use and disclosure for coordinated care. Disclosing information to multiple CE providers that are assisting to connect the individuals to appropriate resources and services.

- Use and disclosure to determine client prioritization for housing. Disclosing assessment data can help staff determine the placement of an individual on a prioritization list and if needed develop a safe sheltering plan while the individual is waiting for placement into permanent housing.
- Use and disclosure for making referrals. Disclosing client information can help match a person to the right resource and potentially create multiple referral options.
- Use and disclosure for determining participant progress. HMIS can be used to build a single participant record that contains information through the CE process from access to project enrollment.

The confidentiality of HMIS data will be protected. CHOs must collect data by legal and fair means. Clients that provide permission to enter personal information allow for CHOs within the continuum to share client and household data.

Uses and Disclosures with Client Consent

CHOs need written consent to disclose client information for the following reasons:

- To conduct a study or research project approved by the CoC
- When required by law (to the extent that use or disclosure complies with and is limited to the requirements of the law);
- To avert a serious threat to health or safety if:
    - The use or disclosure is reasonably believed to be necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public; and
    - The use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat.

- To report about an individual reasonably believed to be a victim of abuse, neglect, or domestic violence to a governmental authority (including a social service or protective services agency) authorized by law to receive reports of abuse, neglect, or domestic violence in any of the following three circumstances:
    - Where the disclosure is required by law and the disclosure complies with and is limited to the requirements of the law;
    - If the individual agrees to the disclosure; or
    - To the extent that the disclosure is expressly authorized by statute or regulation and either of the following are applicable:
        - The CHO believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or
        - If the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the HMIS data for which disclosure is sought is not intended to be]used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure;
    - When such a permitted disclosure about a victim of abuse, neglect, or domestic violence is made, the individual making the disclosure will promptly inform the individual who is the victim that a disclosure has been or will be made, except if:
        - In the exercise of professional judgment, it is believed that informing the individual would place the individual at risk of serious harm; or
        - It would be informing a personal representative (such as a family member or friend), and it is reasonably believed that the personal representative is responsible for the abuse, neglect, or other injury, and that informing the personal representative would not be in the best interests of the individual as determined in the exercise of professional judgment.
- To a law enforcement official for a law enforcement purpose (if consistent with applicable law and standards of ethical conduct) under any of these circumstances:
    - In response to a lawful court order, court-ordered warrant, subpoena or summons issued by a judicial officer, or a grand jury subpoena;
    - If the law enforcement official makes a written request for HMIS data that:
        - Is signed by a supervisory official of the law enforcement agency seeking the HMIS data;
        - States that the information is relevant and material to a legitimate law enforcement investigation;
        - Identifies the HMIS data sought;
        - Is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and
        - States that de-identified information could not be used to accomplish the purpose of the disclosure.
    - If it is believed in good faith that the HMIS data constitutes evidence of criminal conduct that occurred on the CHO's premises;
    - In response to an oral request for the purpose of identifying or locating a suspect, fugitive, material witness or missing person and the HMIS data disclosed

consists only of name, address, date of birth, place of birth, social security number and distinguishing physical characteristics; or
    - If the official is an authorized federal official seeking HMIS data for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879 (threats against the President and others), and the information requested is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought.
- To comply with government reporting obligations for HMIS and for oversight of compliance with HMIS requirements.
- To third parties for the following purposes:
    - To permit other systems of care to conduct data matches (i.e., to determine if you are also utilizing services from such other systems of care); and
    - To permit third party research firms and/or evaluators to perform research and evaluation services, as approved by the CoC, relating to the projects administered by the HMIS Lead and the CHOs;
    - Provided that before client-level HMIS data are disclosed under this subsection, the third party that will receive such client-level HMIS data and use it as permitted above must first execute a Data Use and Security Agreement. The Data Use and Security Agreements requires the third party to comply with all applicable laws and regulations, including the privacy standards and disclosure provisions contained in the current HUD HMIS Data and Technical Standards.

The HMIS Lead may share client level HMIS data with contracted entities as follows:

- The CHO originally entering or uploading the data to the Texas Balance of State HMIS.
- Outside organizations under contract with the HMIS Lead Agency or other entities acting on behalf of the Texas Balance of State CoC for research, data matching, and evaluation purposes. The results of this analysis will always be reported in aggregate form; client level data will not be publicly shared under any circumstance.

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.

Client Consent Refusal Procedures

Client consent refusal should be documented in the appropriate space on the Release of Information document. If client refuses consent, the end user should change the Security Restriction setting in HMIS to “Restrict to Organization.”

CHOs shall uphold Federal and State Confidentiality regulations and laws that protect client records. If the client refuses consent, they are still eligible to receive assistance and services from the CHO.

Data Policies and Procedures

Data Retrieval and Sharing

HMIS, as implemented in the Texas Balance of State CoC regions, is a system that will generate reports required by HUD, the CoC, and other stakeholders. This will be at a level that does not identify individuals but can provide accurate statistical data such as numbers served and trend assessments based on data entered by CHOs. Data from HMIS will be used to produce CoC and local level statistical reports as well as corresponding reports.

The HMIS Lead Agency staff has access to retrieve all data in the TX-607 HMIS. The HMIS Lead Agency will protect client confidentiality in all reporting.

CHOs may share clients' personal information with each other for the purposes of determining eligibility and coordinating client services. For other data sharing, indicated in the Client Informed Consent and Privacy Rights section, CHOs may only provide the client's personal information once an agreed upon Release of Information is in place.

CHOs may also retrieve HMIS data entered to produce statistical reports including number of clients served and trend assessments for internal purposes, grant applications, and other required reports, within the parameters established by the HMIS Lead.

Data Quality

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

The HMIS staff will evaluate the quality of CHOs data using the Universal Data Quality Report (UDQ), HMIS reports, and other tools. CHOs must follow the data quality requirements outlined in the HMIS Data Quality Plan.

Baseline Requirement. PPI collected by a CHO must be relevant to the purpose for which it is to be used. To the extent necessary for those purposes, PPI should be accurate, complete and timely.

A CHO must develop and implement a plan to dispose of or, in the alternative, to remove identifiers from, PPI that is not in current use seven years after the PPI was created or last changed (unless a statutory, regulatory, contractual, or other requirement mandates longer retention).

Data Timeliness

All data entry should happen within a set amount of time established by the CoC. Different project types have different data entry time frames that range from one to three days.

Project	Timeframe
Emergency Shelter	• Universal data elements and housing check-in/check-out are entered within **1 business day** &

	• Assessment entered within **1 business day** of enrollment.
Homeless Prevention & Rapid Re-Housing	Universal Data Elements/Assessments are entered within **1 business day** of enrollment.
Transitional and Permanent Supportive Housing	Universal Data Elements and Housing Check-in/Check-Out entered within **3 business days** of enrollment.
Outreach	• Personally identifiable information (PII) entered within **3 business days** of initial engagement & • Universal Data Elements/Assessment entered within **3 business days** of enrollment.
Supportive Services Only	Universal Data Elements/Assessments entered within **3 business days** of enrollment.

Data Completeness

All data entered into the system should be as complete as possible. It is the CHO's responsibility to ensure that they are asking clients for HUD's Universal Data Elements. Even if the client refuses to answer a specific question, the CHO must at least make the effort to ask in order to create a complete and accurate client record.

Data Accuracy

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

- CHOs must sign the HMIS New Agency Application to ensure that all participating programs are aware and have agreed to the data quality standards.
- Upon agreement, CHOs will collect and enter as much relevant client data as possible for the purposes of providing services to that client.
- The HMIS staff will conduct quarterly checks for data quality. Any patterns of error or missing data will be reported to the CHO.
    - End users will be required to correct the identified data error and will be monitor for compliance by the CHO and the HMIS staff.
- End users may be required to attend additional training as needed.

Data Reporting and Performance Management

A majority of the data entered into the CoC's HMIS directly impacts large scale, HUD-mandated reports such as the System Performance Measures (SPMs) and the Longitudinal System Analysis (LSA). These reports can potentially impact the CoC's funding, which could in turn impact individual CHOs' funding.

Because of this, the CoC has expectations for CHOs in terms of data entry and data quality. The CoC also expects CHOs to participate in quarterly data quality checks known as the Universal Data Quality Report. This quarterly data check acts as the CoC's overarching performance and data quality management. The CoC may also ask individual CHOs to run

other types of reports like a Duplicate Client Report, to check for data quality. The CoC encourages CHOs to run these reports in between quarters as well.

CHOs should check for data entry errors like duplicate enrollments, duplicate clients, missing assessments, incorrect project start and end dates, missing Universal Data Elements, and destinations that are set to "Other."

Federally funded CHOs are expected to submit their APRs or CAPERs to HUD on time. The CoC will provide technical assistance to the CHO as needed to generate these reports. More Information can be found in the Data Quality Plan.

Report	Who Runs It	Suggested Run Times	Due Dates
Universal Data Quality Report	The CoC & All CHOs	Quarterly; based on fiscal year beginning October 1st	Quarterly
Duplicate Client Report	All CHOs	Quarterly; based on fiscal year beginning October 1st	N/A
CAPER	ESG-Funded CHOs	Quarterly	Dependent on funding source
APR	CoC-Funded CHOs	Quarterly	Dependent on funding source
SPMs	The CoC	Quarterly	Late May
LSA	The CoC	At the end of the calendar year	Early August

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.

- CHOs may use data contained in the system to support the delivery of services to homeless clients in the continuum. Agencies may use or disclose client information internally for administrative functions, technical support, and management purposes. CHOs may also use client information for internal analysis, such as analyzing client outcomes to evaluate program.
- The vendor and any authorized subcontractor shall not use or disclose data stored in HMIS without expressed written permission in order to enforce information security protocols. If granted permission, the data will only be used in the context of interpreting data for research and system troubleshooting purposes. The Service and License Agreement signed individually by the HMIS Lead Agency and vendor contain language that prohibits access to the data stored in the software except under the conditions noted above.

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.

- No identifiable client data will be released to any person, agency, or organization for any purpose without written permission from the client.
- 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.

Resources

- HMIS New Agency Application
- HMIS User Agreement
- HMIS Admin Agreement
- HMIS Client Release of Information
- HMIS Privacy Policy
- HMIS Privacy Notice