Connecticut Homeless Management Information System
Policies and Procedures Manual

Version 6: Revised June 2022

Approved by CT HMIS Steering Committee September 9, 2022

The Connecticut Homeless Management Information System (CT HMIS) is managed by the Connecticut Coalition to End Homelessness. For further information about the CT HMIS contact:

Connecticut Coalition to End Homelessness

257 Lawrence Street

Hartford, CT 06106

Phone: (860) 721-7876

www.cceh.org

Table of Contents

Section 1: Contractual Requirements and Roles

Section 1: Contractual Requirements and Roles

Written: 10/2005
Revised: 06/2022
Approved: 09/09/2022

Policy 101: CT HMIS Contract Requirements

Policy:

The CT HMIS Lead Agency is tasked with coordination and provision of data management services to Homeless programs, including emergency shelter, transitional and supportive housing programs, and other HUD or federal partner funded programs such as RHY, PATH, VA, HOPWA, etc. that are required to participate in a CT HMIS. Participating Agencies shall sign a Memorandum of Understanding and comply with the stated requirements.

Procedure:

The CT HMIS Lead Agency will contract for and administer a contract for a fully functional and secure HMIS, which may include a CT HMIS System Administrator who will also be bound by these policies and procedures.

Participating HMIS Agencies shall sign a Memorandum of Understanding and comply with the stated requirements. Participating Agencies will be granted access to the CT HMIS software system after:

- The Memorandum of Understanding (MOU) has been signed with CT HMIS Lead Agency, and
- Participating Agencies have put into place the stated requirements in the MOU.

Agencies agree to comply with the policies and procedures approved by the CT HMIS Steering Committee.

Section 1: Contractual Requirements and Roles

Policy 102: CT HMIS Steering Committee

Written: 10/2005
Revised: 06/2022
Approved: 09/09/2022

Policy:

A Steering Committee, convened by CT HMIS Lead Agency, representing stakeholders to this project, will advise all project activities. The committee meets on a schedule it determines. A current CT HMIS Steering Committee Membership List may be obtained from CT HMIS Lead Agency.

The CT HMIS Steering Committee guides this project, serves as the decision-making body and provides advice and support to the CT HMIS Lead Agency staff.

Procedure:

The CT HMIS Steering Committee will take actions that ensure adequate privacy protection provisions in project implementation.

Membership of the CT HMIS Steering Committee will be established according to the following guidelines:

- Each Coordinated Access Network (CAN) will appoint two individuals, one primary and one alternate, who will represent their members and communicate back to them.
- Each CAN is responsible to find a replacement for any representative that is participating inconsistently or is inactive.
    - CT HMIS SC by-laws include additional information about attendance requirements.
- The CT HMIS Steering Committee has the authority to add non-voting members from other sectors of the community in a method it deems appropriate.
- CANs should consider individuals who have a “big picture” view of the state homeless services system and CT HMIS and some knowledge of one or more of the following when deciding on appointments to the CT HMIS SC. CANs should seek to appoint representatives who have different expertise/qualifications from each other:
    - Privacy protections
    - HUD HMIS Data Standards
    - Client rights
    - Data security
    - Data Quality
    - Knowledge of CT HMIS program types and how their needs interact
    - Lived experience of homelessness
    - Technology
- People with the following roles/ functions should be considered when making appointments
    - Director/Lead of Quality Assurance
    - Director of Programs (a person who oversees many programs within an organization)

The responsibilities and decision-making authority of the CT HMIS SC are outlined in the CT HMIS SC by-laws.

Responsibilities of HMIS SC Members:

- Serve as a liaison between CAN and CT HMIS SC
- Report back to their CAN on CT HMIS SC decisions
    - At minimum share CT HMIS SC meeting minutes at CAN meetings
- Provide information on items requiring quorum votes to the CAN and vote based on CAN decisions related to those items
- Provide input from the CAN to the CT HMIS SC on various topics
- Coordinate with alternate to ensure the CAN attendance at ad hoc meetings

Section 1: Contractual Requirements and Roles

Policy 103: CT HMIS Management

Written: 10/2005
Revised: 06/2022
Approved: 09/09/2022

Policy:

The Executive Director of the CT HMIS Lead Agency is responsible for oversight of all contractual agreements with funding entities, and the CT HMIS organization's adherence to the guiding principles, as determined by the CT HMIS Steering Committee.

Procedure:

- The CT HMIS Steering Committee holds the final authority for all decisions related to the statewide governance of the CT HMIS.
- CT HMIS Lead Agency is responsible for the day-to-day operation and oversight of the system and the CT HMIS Steering Committee grants CT HMIS Lead Agency the authority to act on its behalf to address operational and system level concerns as they arise.
    - This authority may be delegated to third parties at the discretion of CCEH management.
    - Decisions made or actions authorized by CT HMIS Lead Agency which do not satisfy an interested party, which may be a participating agency orgencies, prospective participating agency, or consumers, may be brought before the CT HMIS Grievance Committee for review in accordance with the CT HMIS Grievance Procedure. (See Grievance Procedure policy and forms pages)

CT HMIS Lead Agency responsibilities for the operation and oversight of the system include:

- Management of technical infrastructure;
- Planning, scheduling, and meeting statewide project objectives;
- Coordinating training and technical assistance including an annual series of training workshops for licensed end users, agency administrators; and
- Implementing software enhancements approved by the CT HMIS Steering Committee.

Section 1: Contractual Requirements and Roles

Policy 105: CT HMIS Security Officer

Written: 07/2013
Revised: 06/2022
Approved: 09/09/2022

Policy:

The CT HMIS Lead Agency must designate a CT HMIS Security Officer. Each Participating Agency must designate an Agency Security Coordinator who is responsible for ensuring each Participating Agency is meeting the minimum security requirements established in the Security Plan and the CT HMIS Participating Agency Memorandum of Understanding and is authorized by the Executive Director or Designee of the Participating Agency to provide verification of that status.

Procedure:

The CT HMIS Security Officer is named by the CT HMIS Lead Agency. The duties of the Security Officer must be included in the individual's job description. These duties include, but may not be limited to:

- Cooperatively with the CT HMIS Administrator, review the Security Plan annually and at the time of any change to the security management process, the system software, the methods of data exchange, and any HMIS data or technical requirements issued by HUD. In the event that changes are required to the CT HMIS Security Plan, work with the CT HMIS Administrator to develop recommendations to the CT HMIS Steering Committee for review, modification, and approval.
- Annually review the CT HMIS Security Plan, test the CT HMIS security practices for compliance, and work with the CT HMIS Administrator to coordinate communication with the CT HMIS System Administrator(s) to confirm security compliance of the system.
- Using the CT HMIS Security Plan, certify that the CT HMIS Lead Agency adheres to the Security Plan or develop a plan for mitigating any shortfall, including milestones to demonstrate elimination of the shortfall over as short a period of time as is possible.
- Implement any approved plan for mitigation of shortfalls and provide appropriate updates on progress to the CT HMIS Steering Committee.
- Respond, in cooperation with the CT HMIS Administrator, to any security questions, requests, or security breaches.
- Work with the CT HMIS System Administrator to communicate and interact collaboratively with the Agency Security Coordinators.

Section 1: Contractual Requirements and Roles

Policy 106: Participating Agency Responsibility

Written: 10/2005
Revised: 06/2022
Approved: 09/09/2022

Policy:

Each CT HMIS Participating Agency will be responsible for oversight of all agency staff that generate or have access to consumer-level data stored in the system software to ensure adherence to HIPAA and all State and Federal regulations as well as to ensure adherence to the CT HMIS principles, policies and procedures outlined in this document.

Procedure:

The CT HMIS Participating Agency:

- Holds final responsibility for the adherence of the agency's personnel to The Health Insurance Portability and Accountability Act of 1996 (HIPAA), if applicable, and all State and Federal regulations as well as ensuring compliance with the CT HMIS principles, CT HMIS policies and procedures, and the CT HMIS MOU;
- Is responsible for all activity associated with agency staff access and use of the CT HMIS data system;
- Is responsible for establishing and monitoring agency procedures that meet the criteria for access to the CT HMIS System, as detailed in the policies and procedures outlined in this document and the Participating Agency MOU;
- Will have established policies and procedures to prevent any misuse of the software system by designated staff;
- Agrees to allow access to the CT HMIS System only to staff who have been trained in the CT HMIS system and who have a legitimate need for access. Need exists only for those designated personnel and/or volunteers who work directly with (or who supervise staff who work directly with) consumers, or have data entry or technical responsibilities;
- Agrees to follow approved policies and procedures as approved by the CT HMIS Steering Committee;
- Oversees the implementation of data security standards;
- Assumes responsibility for integrity and protection of consumer-level data entered into the CT HMIS system;
- Ensures organizational adherence to the CT HMIS Policies and Procedures;
- Assigns staff to serve as Agency Security Coordinator and CT HMIS Data Coordinator (HDC);
    - Agency Security Coordinator and/or HDC will effectively communicate system requirements and changes to Agency Licensed End Users;
- Authorizes system access to agency staff;
- Monitors compliance and periodically review data quality and completeness;
- Ensures that data is collected in a way that respects the dignity of the consumers;

- Ensures that all required data is collected and entered accurately and on time (timeliness is determined by HUD and other funders, and varies by program type);
- Provides prompt and timely communications of data, changes in license assignments, and user accounts and software to the CT HMIS Systems Administrator; and
- Notifies Director of HMIS and Strategic Analysis of any issue relating to system security or consumer confidentiality by phone or email immediately upon discovery of incident on a timely basis and using the Security Alert Reporting Form for CT HMIS.

Section 1: Contractual Requirements and Roles

Policy 107: Participating Agency HMIS Data Coordinator

Written: 10/2005
Revised: 06/2022
Approved: 09/09/2022

Policy:

Every Participating Agency must designate one person to be the HMIS Data Coordinator (HDC) who holds responsibility for the coordination of the system software in the agency.

Procedure:

The HMIS Data Coordinator will be responsible for duties including:

- Becoming a CT HMIS licensed end user with a "HMIS Data Coordinator" role.
- Act as liaison between the participating agency and the CT HMIS Lead Agency and CT HMIS System Administrator.
- Ensure, to the extent possible, that all agency and program data is entered accurately and on time according to all contractual requirements.
- Facilitate timely reporting from the agency they represent (unless the agency has designated another person for this function) reports such as;
    - DSS Emergency Shelter Utilization Report
    - DSS AIDS Funded Program Report
    - HUD Annual Performance Report (APR)
    - Data Quality Reports etc.
- Ensure that all agency staff who will be using HMIS:
    - Receive authorized HMIS training
    - Satisfactorily demonstrate proficiency in use of the software
    - Understand the Policies and Procedures that apply to their role in the system.
- Designate each individual's level of access by submitting a Designation of Access (DOA) form to CT HMIS System Administrator.
- Notify CT HMIS System Administrator when a CT HMIS licensed end user leaves the agency or no longer requires access to the CT HMIS system.
- Grant technical access to CT HMIS for agency staff as needed.
- Keep agency and program information up to date. This includes but is not limited to, location, services provided, HUD requirements, and bed inventories (for housing programs).
- Notify all licensed end users in their agency of interruptions in service, changes to data entry workflow, reporting requirements, and upcoming trainings.
- Attend monthly HMIS Data Coordinator meeting held by CT HMIS System Administrator.

The following responsibilities may be performed by the Agency Security Coordinator or the HDC, who may be the same individual:

- Assume responsibility for the integrity and protection of consumer-level data by following the policies outlined for the project, which include but are not limited to:

  - Consumer CT HMIS Consent and Release of Information Forms are signed and on file, Forms can be found at: https://www.cthmis.com/info/detail/general-hmis-info/23
  - Interagency agreements are signed and on file (when applicable);
  - Ensure that the proper IT controls are in place for network, desktop and user security;
- Run CT HMIS User Access report on a quarterly basis
  - See CT HMIS User Access Report Procedures for additional information

CT HMIS Lead Agency will coordinate training and technical assistance for HMIS Data Coordinators.

Section 1: Contractual Requirements and Roles

Policy 108: Agency Security Coordinator

Written:
Revised: 06/2022
Approved: 09/09/2022

Policy:

Every Participating Agency must designate one person to be the Agency Security Coordinator who is an individual designated by each Agency as responsible for ensuring that the Agency meets and maintains local HMIS security standards. The Agency Security Coordinator and the HMIS Data Coordinator may be, but are not required to be, the same person.

Procedure:

The Agency Security Coordinator will ensure Participating Agency compliance with the administrative requirements as listed in the CT HMIS Memorandum of Understanding, Section B Attachments.

The Agency Security Coordinator oversees the implementation of data security policies and standards and will:

- Assume responsibility for integrity and protection of consumer-level data entered into the CT HMIS system;
- Ensure organizational adherence to the CT HMIS Policies and Procedures;
- Authorize data access to agency staff and assign responsibility for custody of the data;
- Monitor compliance and periodically review data security;
- Ensure that data is collected in a way that respects the dignity of the participants;
- Ensure that all data collected must be relevant to the purpose for which it is used, that the data is entered accurately and on time;
- Provide prompt and timely communications of data, changes in license assignments, and licensed end user accounts and software to the CT HMIS System Administrator;
- Notify CT HMIS Lead Agency staff of any issue relating to system security or consumer confidentiality.
- Communicate any security questions, requests, or security breaches to the CT HMIS System Administrator and CT HMIS Security Officer, and security-related HMIS information relayed from CT HMIS Lead Agency to the agency's licensed end users.
- Complete security training offered by the CT HMIS System Administrator. Additional duties that may be incorporated in the CT HMIS Agency Memorandum of Understanding on a case-by-case basis include:
    - Provide security training to the agency's licensed end users based on Security training provided to the Agency Security Coordinator by the CT HMIS System Administrator.

The CT HMIS Lead Agency will coordinate training and technical assistance for Agency Security Coordinators.

Agency Procedure: Each Agency will provide the name and contact information of the Agency Security Coordinator at least annually in the Security Certification checklist. Changes to the individual named as the Security Contact that occur during the course of the year will be communicated via email to the CT HMIS System Administrator and CT HMIS Security Officer within thirty days of the change.

The CT HMIS Security Officer will maintain the name and contact information of the current Agency Security Coordinator of each Agency on file. This file is considered part of the CT HMIS Security Plan and is incorporated by reference.

Section 1: Contractual Requirements and Roles

Policy 109: Licensed End User

Written: 10/2005
Revised: 06/2022
Approved: 09/09/2022

Policy:

All individuals at the CT HMIS Lead Agency, CT HMIS System Administrator, and at the Participating Agency levels who require legitimate access to the software system will be granted such access after training and agency authorization. Individuals with specific authorization can access the system software application for the purpose of conducting data management tasks associated with their area of responsibility.

Procedure:

- The CT HMIS Systems Administrator agrees to authorize use of the CT HMIS only to licensed end users who have received appropriate training, and who need access to the system for technical administration of the system, report writing, data analysis and report generation, back-up administration or other essential activity associated with carrying out CT HMIS responsibilities.
- The Participating Agency agrees to authorize use of the CT HMIS only to licensed end users who need access to the system for data entry, editing of consumer records, viewing of consumer records, report writing, administration or other essential activity associated with carrying out participating agency responsibilities.

Licensed End User Requirements:

- Licensed End Users are any persons who use the CT HMIS software. They must be aware of the data's sensitivity and take appropriate measures to prevent unauthorized disclosure.
- Licensed End Users are responsible for protecting institutional information to which they have access and for reporting security violations.
- Licensed End Users must comply with the data security policy and standards as described and stated by the Agency.
- Licensed End Users must stay current with software modifications, policy and procedure updates, and security protocols.
- Licensed End Users are expected to work collaboratively with HMIS Data Coordinators and Agency Security Coordinators, to maximize system functionality and data accuracy and relevance.
- Licensed End Users are accountable for their actions and for any actions undertaken with their usernames and passwords. Licensed End Users must advise the Agency Security Coordinator, HMIS Data Coordinator (and/or CT HMIS System Administrator) if their passwords are compromised.
- Licensed End Users must not share user IDs, email addresses, or passwords for CT HMIS accounts or contact points for Multi-Factor Authentication.

  - If a user is found to be sharing an email address they and their HDC will be notified and their account will be deactivated if a unique email is not provided within 2 weeks.
- Contractors, volunteers, interns and others who function as staff, whether paid or not, are bound by the same Licensed End Users responsibilities and rules set forth in this manual.

Section 1: Contractual Requirements and Roles

Policy 110: Training Schedule

Written: 10/2005
Revised:
Approved:

Policy:

The CT HMIS Lead Agency will coordinate training for licensed end users of the system. The CT HMIS Lead Agency may contract with the CT HMIS System Administrator or other entities that are qualified to provide the appropriate training. Different levels of training are required for level of access and roles such as Systems Administrators, HMIS Data Coordinators, Agency Security Coordinators and Licensed End Users. Training will occur on a regular basis. The schedule of trainings will be published by the CT HMIS Lead Agency.

Procedure:

All system users must have a license and have successfully completed training that is required for the level of access prior to use of the system.

Section 1: Contractual Requirements and Roles

Policy 111: Amending Policies and Procedures

Written: 10/2005
Revised: 06/2022
Approved: 09/09/2022

Policy:

These Policies and Procedures may be amended. It is expected that information will be added, removed and altered as necessary. The policies will be reviewed every three years.

Procedure:

Each Continuum of Care has representation on the CT HMIS Steering Committee through members of each Coordinated Access Network. Any changes suggested by any party in the Continuum may be presented by a member of the CT HMIS Steering Committee or any CT HMIS Lead Agency staff member to the CT HMIS Steering Committee. Suggestions will be handled and recommendations for action will be made according to the CT HMIS Steering Committee procedure for voting on changes to policies and procedures.

Section 1: Contractual Requirements and Roles	Written: 07/2013 Revised:
Policy 113: Disaster Recovery Plan	Approved:

Policy:

The CT HMIS System Administrator will maintain a current Disaster Recovery Plan.

Procedure:

The CT HMIS Steering Committee will set a schedule and procedures for reviewing the Disaster Recovery Plan.

Section 1: Contractual Requirements and Roles

Policy 114: Grievance Policy

Written: 06/2022
Revised:
Approved: 09/09/2022

Policy:

Grievance by clients[1]

Clients of participating agencies use the participating agency's existing grievance procedure regarding unsatisfactory services or use and disclosure of Personal Protected Information (PPI) in HMIS. If concerns about use of PPI cannot be resolved at the agency level the subcommittee of the CT HMIS SC will consider the grievance. Client grievances related to system-level concerns, issues not specific to a participating agency, will also be considered by the grievance subcommittee.

Grievance by Participating Agencies or a Continuum of Care

If a Participating Agency, prospective Participating Agency, or Continuum of Care has a complaint about a decision or action of the HMIS Lead Agency staff concerning HMIS Governance, Administration, End-User Administration & Support, Data Maintenance and Access, Compliance and Monitoring, Reporting, Project Management, Planning and Policy Development, HMIS Grant Application & Administration, Data Quality, Compliance Monitoring, or Project Evaluation, they should first bring the matter to the attention of the Director of HMIS and Strategic Analysis, and/or the designee who has the ability and authority to take corrective action, as a verbal or informal Grievance Procedure.

Procedure:

Informal Grievance Procedure

The informal grievance procedure involves bringing the issue verbally to the HMIS Lead Agency staff that has the ability and authority to take corrective action. It is intended that discussion between the parties shall resolve the issues.

Formal Grievance Procedure

If the matter is not resolved through the Informal Grievance Procedure to the satisfaction of the Participating Agency or Continuum of Care the Formal Grievance Procedure should be initiated.

1. The complaint should be in writing and submitted to the Director of HMIS and Strategic Analysis

2. If the grieving party is not satisfied, the decision may be appealed to a grievance subcommittee of the CT HMIS Steering Committee who will hear and resolve the complaint at its next regularly scheduled meeting.

[1] Policies adapted from https://irp-cdn.multiscreensite.com/2d521d2c/files/uploaded/HMIS%20Docs%20-%20Client-Grievance-Policy-Final.pdf

Section 2: Participation Requirements

Section 2: Participation Requirements

Policy 201: Participation and Implementation Requirements

Written: 10/2005
Revised: 06/2022
Approved: 09/09/2022

Policy:

In order to participate in CT HMIS, Participating Agencies must sign the CT HMIS Memorandum of Understanding (MOU), meet the minimum criteria stated within the MOU, and comply with the CT HMIS Policies and Procedures.

Procedure:

Participating Agencies are responsible for the following responsibilities whether carried out by Participating Agency employees or by a contractor retained by the Participating Agency:

- Compliance and self-certification thereof, with all policies, procedures and agreements through mechanisms established by the CT HMIS Steering Committee (see CT HMIS Memorandum of Understanding, Exhibits A and B)
- Collecting and entering data into CT HMIS as per these policies and procedures
- Ensuring licensed end users of the program level HMIS compliant system are adhering to the privacy and confidentiality requirements
- Ensuring licensed end user participation in trainings
- Assigning qualified personnel to support initiatives such as the ECM software implementation in the event of transition to a different software vendor
- Produce all necessary HUD reports, e.g. APR, ESG.

The CT HMIS Lead Agency or its designee will monitor Participating Agency compliance with these policies and procedures and can verify Self-Certifications via requests for documentation. Participating Agencies must self-certify that Administrative and Security Checklist requirements are met.

Section 2: Participation Requirements

Policy 202: CT HMIS Lead Agency Data Security Responsibility

Written: 10/2005
Revised: 06/2022
Approved: 09/09/2022

Policy:

The CT HMIS Lead Agency will manage the contractual relationship with a third party software vendor who will in turn continue to develop, implement and maintain all components of operations of the web-based system including a data security program.

Procedure:

The CT HMIS Lead Agency, in consultation with the CT HMIS Steering Committee, will develop the Security Plan, implement its standards; and require compliance with the plan.

Access to areas containing statewide CT HMIS equipment, data, and software will be secured. All client-identifying information will be strictly safeguarded in accordance with appropriate technical safeguards. All data will be securely protected to the maximum extent possible.

Ongoing security assessments to include penetration testing will be conducted on a regular basis.

The scope of security includes:

- Technical safeguards including:
    - Multi Factor Authentication with the following requirements;
        - Multi-factor Authentication (MFA) re-authentication will be required weekly.
        - Users cannot share mobile or email accounts to receive MFA codes.
            - CT HMIS System Administrator will audit accounts on a quarterly basis
            - Any users that are found to have a shared mobile number and/or email address set up for MFA communication will be notified along with their HDC and given 2 weeks to provide unique email/mobile number
            - If a unique contact is not provided the account will be deactivated
- Physical safeguards, including, but not limited to locked doors;
- Network protocols and encryption standards such as https/ssl encryption (an indicator of encryption use); and
- Client data security (Data Encryption).

A CT HMIS Security Officer will be assigned by the CT HMIS Lead Agency to monitor the CT HMIS Security Plan and monitor compliance by Participating Agencies and Licensed End Users, in collaboration with the CT HMIS System Administrator.

Section 2: Participation Requirements	Written: 10/2005
	Revised: 07/2021
Policy 205: Statewide Data Sharing Requirement	Approved:

Policy:

Multiple funders of programs that provide services to homeless individuals and families require a standardized data collection system (HMIS). HUD and other funders mandate data sharing among Participating Agencies. CT HMIS is compliant with this requirement and all Participating Agencies must follow data sharing policy and procedures. In addition, Participating Agencies must follow Privacy and Informed Consent procedures as outlined in relevant policies.

Procedure:

Participating Agencies must ensure that all Licensed End Users are aware of the Statewide Data Sharing Requirement and understand the benefits and need for confidentiality, inform consumers of their options and have the proper internal policies and procedures to protect consumer data.

Participating Agencies must inform each consumer whose record is included in the CT HMIS that data in the system is shared. Each consumer must authorize the inclusion of their information in the system through the written consumer consent and release of information form or by verbally consenting to have data shared at the level they determine. Consumer consent and privacy policies must be followed. Available under the Forms section at:
https://www.cthmis.com/info/detail/general-hmis-info/23

Section 2: Participation Requirements	Written: 10/2005 Revised: 06/2022 Approved: 09/09/2022
Policy 207: Confidentiality, Informed Consent to Enter Data, and System Wide Release of Information	

Policy:

Each consumer must authorize the inclusion of their information in the CT HMIS system by verbally consenting or through the written consumer consent and release of information form. This authorization determines the level of data to be included and shared.

Procedure:

Informed Consent: Includes both a verbal explanation and written or verbal consumer consent for each consumer.

Verbal Explanation: All consumers will be provided a verbal explanation of CT HMIS. The Participating Agency will provide a verbal explanation of CT HMIS and the terms of consent. The agency is responsible for ensuring that this procedure takes place prior to every consumer interview. The verbal explanation must contain the following information:

1. Explanation of CT HMIS:
    a. Computer based information system that homeless services agencies across the state use to capture information about the persons they serve
2. Why the agency uses it:
    a. To understand their consumers' needs
    b. Help the programs plan to have appropriate resources for the people they serve to inform public policy in an attempt to end homelessness
    c. Federal mandate that all HUD funded homeless providers must enter data into an electronic system and capture universal data elements
3. Security
    a. Only staff who work directly with consumers or who have administrative responsibilities can look at, enter, or edit consumer records
4. Privacy Protection
    a. No information will be released to another agency without written consent
    b. Consumer has the right to not answer any question, unless entry into a program requires it
    c. Consumer information is transferred in an encrypted format to CT HMIS
    d. Consumer has the right to know who has added to, deleted, or edited their CT HMIS electronic record
    e. Consumer has the right to receive copies of their HMIS record from the agency that created the record. CAN level records, defined as those created under a specific CAN organization may be requested from the CAN backbone agency. For example: a client who received services from the Greater Hartford CAN may request HMIS records related to their CAN enrollment from Journey Home.

   f. The participating agency must consider any request by a client for correction of inaccurate or incomplete information pertaining to that client. A participating agency is not required to remove any information but may, alternatively, mark information as inaccurate or incomplete and supplement it with additional information

5. Benefits for consumers.
   a. Case manager tells consumer what services are offered on site or by referral through the assessment process
   b. Case manager and consumer can use information to assist consumers in obtaining resources that will help them find and keep permanent housing

Written Consumer Consent to Enter Data:

Each consumer must provide written permission to authorize the agency to enter information into CT HMIS unless initial interaction with a client is by phone, in which case verbal consent is acceptable. The current ROI is available under the Forms section at: https://www.cthmis.com/info/detail/general-hmis-info/23

Written Consumer Release to Share Data:

Each Consumer whose record is being shared electronically with another Participating Agency must agree via a written consumer release of information form to have their data shared. A consumer must be informed what information is being shared and with whom it is being shared. A consumer must also be informed of the expiration date of the consent.

Verbal Consent and Release of Information for telephone-based resource access:

Information Release: The Participating Agency agrees not to release consumer identifiable information to any other organization pursuant to federal and state law without proper consumer consent.

Federal/State Confidentiality Regulations: The Participating Agency will uphold Federal and State Confidentiality regulations to protect consumer records and privacy. In addition, the Participating Agency will only release consumer records with written consent by the consumer, unless otherwise provided for in the regulations.

1. The Participating Agency will abide specifically by the Federal confidentiality rules regarding disclosure of alcohol and/or drug abuse records.
2. The Participating Agency will abide specifically by State of Connecticut general laws providing guidance for release of consumer level information including who has access to consumer records, for what purpose and audit trail specifications for maintaining a complete and accurate record of every access to and every use of any personal data by persons or organizations.

Encryption: The Participating Agency understands that all consumer identifiable data is to be made inaccessible to unauthorized users. Client level information in any format must be sent via encrypted email to maintain confidentiality and policies for maintaining confidentiality should be followed before transmitting any client level information.

Section 2: Participation Requirements

Policy 208: Information Security Protocols

Written: 10/2005
Revised: 06/2022
Approved: 09/09/2022

Policy:

To protect the confidentiality of the data and to ensure its integrity at the site whether during data entry, storage and review or any other processing function, at a minimum, a Participating Agency must develop and have in place appropriate rules, protocols or procedures.

Procedure:

Participating Agency rules, protocols or procedures must address each of the following:

- Assignment of user accounts
- Unattended workstations
- Physical access to workstations
  - The implementation of hardware and/or software firewall to secure local systems/networks from malicious intrusion.
- Use of Antivirus Software, including the automated scanning of files as they are accessed by users on the system where the HMIS application is housed as well as assuring that all consumer systems regularly update virus definitions from the software vendor.
- Password complexity, expiration, and confidentiality
- Policy on licensed users access which includes not sharing accounts
- Consumer record disclosure, confidentiality and release of information
- Report generation, disclosure and storage
- Maintenance and monitoring of all system access logs for systems which have access to HMIS data.
  - Participating Agencies should discourage use of personal computers to access CT HMIS unless managed under the organization’s IT group policies and meeting the above requirements. Storing client level data on personal computers or other personal media (flash drives, external hard drives, etc.) is prohibited.
- Additional requirements as established by the CT HMIS Steering Committee.

Each Participating Agency will participate in annual compliance reviews conducted by the CT HMIS System Administrator.

Section 2: Participation Requirements

Policy 210: Compliance Review

Written: 07/2013
Revised:
Approved:

Policy:

Each Participating Agency will participate in annual compliance reviews conducted by the CT HMIS System Administrator.

Procedure:

Each Participating Agency will participate in the Annual Administrative Certification Process. This may include a completed and certified Annual Administrative Certification Checklist, attached in the CT HMIS Memorandum of Understanding as Exhibit A; and Annual Security Certification Checklist, attached in the CT HMIS Memorandum of Understanding as Exhibit B.

- Agencies seeking first-time access to CT HMIS will be granted access to CT HMIS when all Administrative and Security requirements as outlined in Exhibits A and B have been self-certified as being met.
- Agencies established on CT HMIS that in any given year are unable to self-certify that all requirements are met will be engaged in a 45-60 day remediation process to correct any shortfall. CT HMIS access will continue during this period.

Any required remediation steps recommended by the CT HMIS System Administrator will be completed in a timely manner by the Participating Agency. The CT HMIS Lead Agency will monitor compliance and remediation steps.

The Participating HMIS Agency shall appoint an HMIS Data Coordinator (HDC) responsible for all duties specified in Exhibit A and any additional relevant duties that may be established by the CT HMIS Steering Committee.

The Agency shall appoint a Participating HMIS Agency Security Coordinator responsible for all duties specified in Exhibit B and any additional relevant duties, such as providing security trainings to Agency staff.

No exceptions can be made for any Agency that has indicated in Exhibit A or B of the CT HMIS Agency Memorandum of Understanding that it does not, at the time of execution of the CT HMIS Agency Memorandum of Understanding, meet all requirements for participation in the CT HMIS. Consistent with CT HMIS Policies and Procedures, Agency shall resolve the issues. First time Agency licensed end users of CT HMIS must resolve the issues in order to be granted access to the CT HMIS system. Agencies that already have access will work with the CT HMIS System Administrator in a 45-60 day remediation process to resolve identified issues.

Section 2: Participation Requirements	Written: 07/2015 Revised:
Policy 211: CT HMIS Retraining	Approved: 07/2015

Policy:

Agencies with CT HMIS licensed end users who are in need of retraining will adhere to the guidelines outlined in the procedure of this policy.

Procedure:

Identification of licensed end users who are in need of retraining is based on the following criteria:

- User has not logged into the system in the first 45 days from their initial training
- User has generated three or more helpdesk tickets about the same or similar issue that is unrelated to system performance in a 60 day period
- User has used four or more hours of help desk support in a month for issues unrelated to system performance
- The CoC may also request a re-train of an agency with consistently low UDE and/or ESG performance

When a retraining is necessary, the user(s) will be notified that they must register and attend the appropriate training for their project type within 45 days. The user(s) agency HDC and Executive Director on record with the CT HMIS System Administrator will also be notified of the request and reason for the retraining.

Noncompliance with registration and completion of a training session within the 45 day timeframe will result in the user(s) CT HMIS access being made inactive.

Section 2: Participation Requirements

Policy 212: CT HMIS No Show Policy

Written: 05/2016
Revised:
Approved: 06/2016

Policy:

CT HMIS trainings are currently provided at no cost to CT HMIS licensed end users or potential licensed end users. Agencies with new staff, or with existing CT HMIS licensed end users who need retraining will adhere to the guidelines outlined in the procedure of this policy.

Procedure:

Definition of “No Show”: A no show occurs when an individual who has registered for an in-person CT HMIS training does not attend and fails to notify the system administrator within 1 full business day in advance of their absence. Training confirmation will be sent from the CT HMIS system administrator and will include the contact information for whom to contact if the individual cannot attend the training for any reason. If there is an extenuating circumstance that prevents someone from attending training, the fee may be waived if the individual’s supervisor alerts the system administrator.

If an individual is a no show for training, their organization will be charged a no-show fee according to the following schedule:

- First occurrence per organization: $50
- Subsequent occurrences: $150 per incident

Monthly, the CT HMIS system administrator will provide the CT HMIS Lead Organization with a list of individuals who were no shows – and the CT HMIS Lead Organization will issue the invoices to the appropriate organizations. Funds collected will generally be used to enhance the CT HMIS training environment and will be allocated by the CT HMIS Data Quality Management sub-Committee of the CT HMIS Steering Committee. If an agency has an outstanding fee for CT HMIS training no-shows for over 60 days, the agency will not be able to register new individuals for CT HMIS trainings until all fees are paid.

Section 3: Data Quality

Section 3: Data Quality

Policy 301: Minimum Required Data Elements

Written: 10/2005
Revised: 06/2022
Approved: 09/09/2022

Policy:

The CT HMIS Steering Committee will identify minimum required data elements that are required for every Participating Agency to complete.

The CT HMIS includes data elements that U.S. Department of Housing and Urban Development (HUD) has identified are required, as documented in the Federal Register. For programs that do not have HUD reporting requirements, HUD states that the standards are optional but recommended for CoC's to obtain consistent information. In addition to the HUD required data elements, there are program-specific data elements that are recommended and may be added to funder reports in the future.

Procedure:

The CT HMIS System Administrator will maintain a current data dictionary, located on the CT HMIS website:

The HMIS Data Standards Manual and Data Dictionary
https://files.hudexchange.info/resources/documents/FY-2022-HMIS-Data-Standards-Manual.pdf

CT HMIS Data Dictionary

https://www.cthmis.com/file_uploads/datadictionary/main.html

The DMHAS DDaP standard file format

https://portal.ct.gov/-/media/DMHAS/EQMI/DDaPstandardfileformatpdf.pdf

The CT HMIS Steering Committee may include additional data elements to facilitate reporting for other programs funded in addition to HUD, by organizations including various state agencies such as DSS, DOH, DHMAS, UNITED WAY, and the CT HMIS itself.

Section 3: Data Quality

Policy 302: Data Quality Management Plan

Written: 10/2005
Revised: 06/2022
Approved: 09/09/2022

Policy:

The CT HMIS has a multi-faceted data quality management strategy.

The CT HMIS Steering Committee is charged with implementing and monitoring the Data Quality Management Plan (DQMP), making recommendations and reporting on a periodic basis. The DQMP will include policies and procedures, indicators and targets, monitoring components and periodic review of the plan itself, on a schedule determined by the sub-committee and approved by the Steering Committee.

Participating Agencies are required to enter data into the system in a timely, complete, and accurate manner. This policy outlines the procedures for adherence to the CT HMIS Data Quality standards including the following elements; Timeliness, Completeness, Accuracy/Consistency, Monitoring, and Incentives/Enforcement.

Participating Agencies are required to designate an HMIS Data Coordinator (HDC) who is trained on the software and how to run and review program level reports (including data quality). The HDC is responsible for adherence to the following Data Quality Standards.

Procedure:

The Data Quality Management Plan includes data quality procedures and can be accessed here: https://cceh.org/wp-content/uploads/2021/10/CT-HMIS-2021-Data-Quality-Management-Plan.pdf

Continuous Improvement:

- Statewide HDC webinars are facilitated each month by the CT HMIS Statewide Administrator; this call focuses on changes to the system and common problems that are reported via the CT HMIS Help Desk and data quality reports.
- The Statewide Lead Agency reviews data on a quarterly basis and will report anomalies as they are discovered to the CT HMIS Steering Committee. The CT HMIS Steering Committee will review and may make the decision to follow the recommendations of the Data Quality Management Committee regarding anomalies.

Section 3: Data Quality	Written: 06/2022
	Revised:
Policy 303: Data Retention Policy	Approved: 09/09/2022

Policy:

When an HMIS record has met the threshold of having no changes in the 7 years since it was first created or last updated, CoCs may either completely delete the entire record, or remove identifiers from the record.

Procedure:

The CT HMIS Lead Agency will work with the CT HMIS system administrator and members of the CT HMIS SC to develop and implement a plan to dispose of or, in the alternative, to remove identifiers from, protected personal information (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). Once the plan is created it will be shared with the CT HMIS Steering Committee for approval. Once the plan is approved data will be disposed of or deidentified once annually.

Section 4: User, Location, Physical, and Data Access

Section 4: User, Location, Physical, and Data Access

Written: 10/2005
Revised: 07/2013
Approved:

Policy 401: Access Levels For Licensed End Users

Policy:

Licensed User Levels are designated by the CT HMIS System Administrator. Licensed User accounts will be created and deleted by the CT HMIS System Administrator with approval by the Participating Agency's Executive Director and/or designee.

Procedure:

CT HMIS Licensed End Users designation is based on the access level a user needs to perform their job responsibilities. The determination of an individual's access level should be need- based.

The Participating Agency will designate a representative to facilitate registering Licensed End Users with CT HMIS. This will either be the HMIS Data Coordinator (HDC) or Agency Security Coordinator.

A Participating Agency must require each member of its staff (including employees, volunteers, affiliates, contractors and associates) to sign a Licensed End User Agreement upon successful completion of CT HMIS training, and to comply with the Licensed End User Agreement requirement.

Section 4: User, Location, Physical, and Data Access

Written: 10/2005
Revised: 07/2013
Approved:

Policy 403: Access to Consumer Paper Records

Policy:

Agencies shall follow their existing policies and procedures and applicable local, state and federal regulations for access to consumer records on paper.

Procedure:

Each agency must secure any paper or other hard copy containing Personally Identifiable Information (PII) that is either generated by or for HMIS, including, but not limited to reports, data entry forms and signed consent forms.

All paper or other hard copy generated by or for HMIS that contains PII must be directly supervised when the hard copy is in a public area. When agency staff are not present, the information must be secured in areas that are not publicly accessible. Written information specifically pertaining to user access (e.g., username and password) must not be stored or displayed in any publicly accessible location. Users are prohibited from storing client-level data on any personally owned media or devices.

Section 4: User, Location, Physical, and Data Access	Written: 08/2015 Revised:
Policy 404: Case Note Deletion in CT HMIS	Approved: 11/2015

Policy:

To protect the integrity of the case notes recorded in the system Participating Agencies do not have the ability to delete case notes after they have been saved. The guidelines outlined in the procedure of this policy are to be adhered to when it is necessary for a case note to be deleted from the system.

Procedure:

Participating Agencies are required to designate an HMIS Data Coordinator (HDC) who is trained on the software and will be the only designee at a Participating Agency who may request the deletion of a case note.

When a case note has been identified by a Participating Agency – the agency staff must work with the HDC to initiate the request for the deletion of the case note. The procedure for requesting a deletion would be handled by the HDC through the CT HMIS Help Desk.

Information to be included in the deletion request is the HMIS ID of the client record the case note is associated with, the date the case note was created, and the reason for the deletion request.

Section 4: User, Location, Physical, and Data Access	Written: 06/2022 Revised:
Policy 405: Release of Data Policy	Approved: 09/09/2022

Policy:

CT HMIS data may be released in aggregate or disaggregated format to aid in research, evaluation, or advocacy. Any data requests that include PII must be submitted using a Data Sharing Agreement (DSA) and approved by the CT HMIS Steering Committee (SC).

Procedure:

Releasing Aggregate Data without PII

The CT HMIS Lead Agency accepts data requests from any source and will return aggregate data with no Personally Identifiable Information (PII). PII includes names, initials, date of birth, phone number, email address, and social security number.

1) Requestors complete the Data Request Form
2) Lead agency staff reviews each variable and parameter requested
3) Lead agency staff meets with requestor
4) Data request is processed and delivered

Releasing Data with PII

1) Requestors submit a data request which includes PII
    - A staff member from the CT HMIS Lead Agency contacts the requestor to confirm that PII is needed and discusses the sensitive nature of HMIS PII data
2) The requestor submits the DSA to CT HMIS Lead Agency
    - DSA includes specific legal and detailed information not included in a routine data request
        - Granular detail on the business need and intent of the data request is required
        - The data transfer protocol must be secure and agreed upon between CT HMIS Lead Agency and the requestor as part of the request
        - If the requestor is conducting an analysis or intends to publish the data they must agree to share the data and draft with CT HMIS Lead Agency and the CT HMIS SC prior to publication to confirm accuracy of the data interpretation
            - Client level data may not be published
        - Data may not be shared with third parties not included in the DSA
3) CT HMIS Lead Agency Reviews the DSA
4) The staff from CT HMIS Lead Agency meets with the requestor
5) CT HMIS Lead Agency meets with members of the HMIS SC for approval of the DSA
    - HMIS SC approves or denies the request
6) The DSA is finalized and executed by CT HMIS Lead Agency
7) CT HMIS Lead Agency processes and delivers the request

Attachments

Attachments	Written:
	Revised:
Procedure for Granting CT Homeless Management Information System (HMIS) Access	Effective: 11/5/2019

1.0 Core Criteria

In order to be considered for access to the CT HMIS, the following criteria must be met:

1.1	The request or need cannot be met with other existing reporting options (e.g., custom data pulls or reports, CTCANDATA.org).
1.2	The request must be for on-going access. One-time access will not be considered.
1.3	The request must be directly related to a funding requirement or a homeless services provider.
1.4	The requestor must have a direct connection or a working relationship with people experiencing homelessness.
1.5	If access to a particular Coordinated Access Network (CAN) is requested, the CAN may participate in the decision.
1.6	The access level (full access, view only, or reporting only) must be reflected in the Memorandum of Understanding (MOU).
1.7	The requestor must participate in HMIS training (currently a requirement for all HMIS licensed end users).
1.8	The requestor's access to HMIS must contribute to the cause of ending homelessness.
1.9	If the requestor is a researcher, the request should be limited to aggregated and de-identified data whenever possible. Note: This may not be possible due to research need to match data to other sources.
1.10	The requestor must be in good standing and not had previous HMIS access that was revoked.

2.0 Criteria That Would Prevent Granting of HMIS Access

2.1	Requesting one-time access only.
2.2	Possibility for high abuse if granted access to homeless client data.

3.0 Data Requested from Requestors

3.1	Purpose of request – to be submitted to CCEH
3.2	How access to HMIS will contribute to the effort to end homelessness
3.3	Identify program/department/staff requesting access and specific level of access (full access, reporting only, view only)

4.0 Process for Granting HMIS Access

4.1	MOU will be used for application. MOU must include specific access granted.
4.2	If applicable to a specific CAN, the CAN leadership will be informed and involved in the vetting and decision process.
4.3	If application meets core criteria, CCEH will work directly with requestor to grant access. If application does not clearly meet core criteria, CCEH will engage the HMIS Steering Committee sub-committee and CAN (if applicable) to vet application.
4.4	Future consideration – development of a portal for outside agencies to access a subset of the HMIS data (TBD)

Attachments	Written:
	Revised:
HMIS User Access Report Procedures	Effective: 11/5/2019

The purpose of the User Access Report is to assure that licensed end users are only reviewing client records within the scope of their access permissions.

Step-by-step instructions to run the report are in the User Report Usage Instructions and available at: https://cceh.org/data-quality/

Documentation of Report Review by HDC:

- HDCs will self-monitor their run and review of the report

Review Process

- Run the report monthly as best practice
  - Quarterly is minimum standard
- Review your licensed end users' access activity by Organization(s)
- Look for unexpected access patterns
  - Examples:
    - Spike in values from one month or quarter to the next
    - High volume of records accessed with no enrollments in the Organization
    - Unexpectedly high volume of records accessed by a user considering their role
    - Unexpectedly high volume of records accessed within a specific date range
    - Unexpectedly high volume of accesses for specific client record(s)
- The HDC may want to craft an internal document that fits their agency's protocols so that their licensed end users will be aware of the process

Unexpected Usage Escalation Process:

Level 1 – HDC notices unexpected usage patterns

- HDCs will review usage with immediate supervisor/manager
  - Human Resources will be notified if appropriate for your agency's protocols

Level 2 – HDC and Manager need more information

- HDC and their manager will submit a ticket to Nutmeg to further review unexpected usage
- Nutmeg will confirm that the data is accurate and assist HDC and manager in assessing the usage

Level 3 – HDC, Manager, and Nutmeg still have concerns about the usage

- CCEH will be contacted by the HDC, and a meeting will be set up for CCEH, Nutmeg, HDC, and the Manager
    - Will determine if inappropriate usage has been identified
        - If inappropriate usage is identified
            - Nutmeg will initiate a process to deactivate the user. Deactivation will not be initiated without review by HDC and manager
            - Manager will determine corrective or disciplinary action needed
            - Manager will document outcome and provide a summary to CCEH to bring to the HMIS Steering Committee

Level 4 – CCEH will notify HMIS Steering Committee

- If inappropriate usage is identified CCEH will notify the HMIS Steering Committee of the situation and outcome
    - X number licensed end users deactivated
    - Reasons for deactivation
    - Additional steps taken
- Notification to the party(ies) whose information was breached will follow the National Conference of State Legislators (NCSL) guidelines for the state of Connecticut: https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

Date	Policy	Change Log	Additional Information
09/09/2022	102	Update language to reflect Coordinated Access Network (CAN) based nature of Steering Committee (SC), remove references to continuum and sub continuums.	
09/09/2022	102	Remove language around CT HMIS SC "decision making authority" as it is duplicative of the by-laws.	
09/09/2022	102	Add reference to member attendance requirements	
09/09/2022	102	Clarify that CT HMIS SC has the authority to add non-voting members to the SC.	
09/09/2022	102	Add guidance for CANs on potential considerations for CT HMIS SC nominees.	
09/09/2022	102	Add information on responsibilities of CT HMIS SC members.	
09/09/2022	103	Clarify language around participating agencies.	
09/09/2022	103	Remove reference to Grievance Committee as the information is in the by-laws.	
09/09/2022	107	Add requirement that HMIS Data Coordinators (HDCs) must be CT HMIS Licensed End Users.	
09/09/2022	107	Clarify that HDC is the liaison between participating agency and CT HMIS Lead Agency and System Administrator. Remove language about "pertinent activity."	
09/09/2022	107	Add requirement that HDC run user access report on a quarterly basis, per procedures created with that report.	
09/09/2022	108	Remove language that is duplicative of HDC policy/role.	
09/09/2022	108	Remove language that is duplicative of MOU.	
09/09/2022	109	Add requirement that users not share accounts that are used for Multi Factor Authentication (MFA) communication and will be deactivated if they don't provide unique contact information.	
09/09/2022	111	Add provision that P&P will be reviewed every 3 years.	
09/09/2022	111	Clarify voting procedures.	Full voting procedures can be found in the CT HMIS SC by-laws
09/09/2022	114	New Policy	

Date	**Policy**	Change Log	**Additional Information**
09/09/2022	201	Clarify that participating agencies are responsible for the requirements whether completed by employee or contractor.	
09/09/2022	201	Remove requirements for site visits to verify self-certification of requirements and replace with requests for documentation.	
09/09/2022	201	Remove requirement to participate in CoC meetings.	It is not within the purview of the CT HMIS SC to require this.
09/09/2022	202	Add procedures related to MFA.	
09/09/2022	207	Add procedures for clients to request copies of the CT HMIS records.	
09/09/2022	207	Add procedure for clients requesting Proposed Changes to their record.	
09/09/2022	207	Clarify that all client level information must be sent via encrypted email.	
09/09/2022	207	Remove reference to “script” for explaining Release of Information to clients.	Procedure contains talking points that should be included when speaking with clients about Release of Information and Consent.
09/09/2022	208	Add language around discouraging use of personal computers to access CT HMIS.	
09/09/2022	302	Remove Data Quality Management Plan language and reference DQMP directly via link.	
09/09/2022	302	Remove reference to Data Quality Management Committee.	Ad hoc committees will be formed to address specific data quality needs or projects.
09/09/2022	303	New Policy	
09/09/2022	405	New Policy	