CONNECTICUT HOMELESS MANAGEMENT INFORMATION SYSTEM (CT HMIS)

POLICIES AND PROCEDURES MANUAL

Version 5.3: Revised August 2018 -

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
Voice :(860) 721-7876
FAX: (860) 257-1148
www.cceh.org

SECTION 1:
CONTRACTUAL REQUIREMENTS AND ROLES

SECTION 1: CONTRACTUAL REQUIREMENTS AND ROLES **Written: 10/2005**
Revised: 07/2013

POLICY 101: CT HMIS CONTRACT REQUIREMENTS **Approved:**

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 funded programs 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 (see Attachments) 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 **Written: 10/2005**
Revised: 07/2013

POLICY 102: CT HMIS STEERING COMMITTEE **Approved:**

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 Continuum and sub-continuum of the Balance of State, will appoint two individuals who will represent their members and communicate back to them.
- Each Continuum/sub-continuum is responsible to find a replacement for any representative that is participating inconsistently or is inactive.
- The CT HMIS Steering Committee has the authority to add representatives from other sectors of the community in a method it deems appropriate.

The CT HMIS Steering Committee has decision making authority in the following areas:

- Determining the guiding principles that should underlie the implementation activities of the CT HMIS, including participating organizations, consumer involvement and service programs;
- Selecting the minimal data elements to be collected by all programs participating in the CT HMIS project;
- Defining criteria, standards, and parameters for the release of aggregate data, aggregated and disaggregated; and
- Approving the software vendor

SECTION 1: CONTRACTUAL REQUIREMENTS AND ROLES **Written: 10/2005**
Revised: 07/2013

POLICY 103: CT HMIS MANAGEMENT **Approved:**

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 Statewide 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 an agency (agencies) or a consumer(s), 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)
- The Grievance Committee members shall be selected on a rotating basis and shall not have a conflict of interest for the grievance they are adjudicating. Membership will consist of one Co-Chair of the CT HMIS Steering Committee, one CT HMIS System Administrator and three CT HMIS Steering Committee members.

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 end users, agency administrators; and
- Implementing software enhancements approved by the CT HMIS Steering Committee.

SECTION 1: CONTRACTUAL REQUIREMENTS AND ROLES **Written: 07/2013**
Revised:
POLICY 105: CT HMIS SECURITY OFFICER **Approved:**

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 Participation Agreement, 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 to the CT HMIS System Administrator and CT HMIS Security Officer, and for communicating security-related HMIS information relayed from CT HMIS Lead Agency to the Participating Agency's Licensed End Users.
- Work with the CT HMIS System Administrator to communicate and interact collaboratively with the Agency Security Coordinators.

SECTION 1: CONTRACTUAL REQUIREMENTS AND ROLES **Written: 10/2005**
Revised: 07/2013

POLICY 106: PARTICIPATING AGENCY RESPONSIBILITY **Approved:**

Policy:

Each 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 Participating HMIS Agency:

- Holds final responsibility for the adherence of the agency's personnel to The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and all State and Federal regulations as well as ensuring adherence to the CT HMIS principles, policies and procedures outlined in this document;
- 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;
- 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 for all changes as identifies by the CT HMIS Lead Agency and/or the CT HMIS Steering Committee;
- Oversee the implementation of data security standards;
- 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;
- Assign staff to serve as Agency Security Coordinator and HMIS Data Coordinator;
- Agency Security Coordinator and/or HMIS Data Coordinator will effectively communicate system requirements and changes to Agency Licensed End Users;
- Authorize system access to agency staff;
- Monitor compliance and periodically review data quality and completeness;
- Ensure that data is collected in a way that respects the dignity of the consumers;
- Ensure 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);
- Provide prompt and timely communications of data, changes in license assignments, and user accounts and software to the CT HMIS Systems Administrator; and

POLICY 106: PARTICIPATING AGENCY RESPONSIBILITY, continued

- Notify CCEH CT HMIS staff of any issue relating to system security or consumer confidentiality on a timely basis and using the Security Alert Reporting Form for CT HMIS (attached).

SECTION 1: CONTRACTUAL REQUIREMENTS AND ROLES **Written: 10/2005**
Revised: 07/2013

POLICY 107: PARTICIPATING AGENCY HMIS DATA COORDINATOR **Approved:**

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:

- Serve as point-person in communicating with 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 she/he represents (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 demonstrated 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 (as provided by, and) to CT HMIS System Administrator.
- Notify CT HMIS System Administrator when a CT HMIS system 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 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
- Inform CT HMIS users and senior management of pertinent activity.
- Ensure agency is prepared for annual site visits

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

POLICY 107: PARTICIPATING AGENCY HMIS DATA COORDINATOR, continued

- 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 (see Attachment) are signed and on file;
    - Interagency agreements are signed and on file (when applicable);
    - Ensure that the proper IT controls are in place for network, desktop and user security;

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

SECTION 1: CONTRACTUAL REQUIREMENTS AND ROLES **Written: 10/2005**
Revised: 07/2013

POLICY 108: AGENCY SECURITY COORDINATOR

Approved:

Policy:
Every Participating Agency must designate one person to be the Agency Security Coordinator who holds responsibility for the coordination of the system software in the agency. 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 (Security Alert Report).

Memorandum of Understanding Attachment B

- Agency has a policy detailing its internal communication practices for HMIS matters consistent with Section 2 of the CT HMIS policies and procedures;
- Agency has a policy for granting access to its agency-level HMIS-compliant system's end users consistent with Section 4 of the policies and procedures;
- The agency has adopted Licensed End User Agreement provided by CT HMIS Lead Agency;
- Licensed End User Agreements are signed and on file for all staff who access the agency-level HMIS-compliant system.
- Agency has a policy for managing the breach of Licensed End User agreements.
- Agreement that meets the minimum standards outlined in Section 3 of the policies and procedures;

POLICY 108: PARTICIPATING AGENCY'S AGENCY SECURITY COORDINATOR, continued

- Each end user has been trained on system use, privacy, security, and data collection requirements consistent with train the trainer sessions provided by the CT HMIS Lead Agency or its Agent, the CT HMIS System Administrator, and the CT HMIS policies and procedures, consistent with Sections 3 and 4 of the policies and procedures.
- Agency is a HIPAA covered entity and has a Privacy Policy that meets HIPAA requirements (you must attach a copy of your HIPAA Privacy Policy).
- Agency is not a HIPAA covered entity and the agency has adopted the minimal standard Privacy Policy provided by the CT HMIS Lead Agency
- Agency is not a HIPAA covered entity and has established a Privacy Policy that otherwise meets the minimum requirements established in Section 2 of the policies and procedures (you must attach a copy of the non-standard Privacy Policy).
- The agency's Privacy Policy is posted on the agency's website.
- A sign including the required language described in Section 2 of the policies and procedures is posted at all intake desks or other location where data collection occurs.
- The agency has a policy requiring that all consumer data is entered into the system within, at most, the timeframe established in CT Data Quality Standards (following the standards required by HUD for HMIS data) as approved and adopted by the CT HMIS Steering Committee
- The agency has a policy for conducting logic checks to validate the accuracy of the data in its program-level HMIS-compliant system and regularly comparing universal and provider program specific data elements to available paper records and updating/correcting missing or inaccurate data, consistent with the CT Data Quality Standards.

Agency Procedure: Each Agency will provide the name and contact information of the Agency Security Coordinator at least annually in the Security Certification document. 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.

- 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.

POLICY 108: PARTICIPATING AGENCY'S AGENCY SECURITY COORDINATOR, continued

- Complete security training offered by the CT HMIS System Administrator. Additional duties that may be incorporated in the Agency Participation Agreement on a case-by-case basis include:

    - Provide security training to the agency's end users based on Security training provided to the Agency Security Coordinator by the CT HMIS System Administrator.
    - Any security-related questions from Agency staff will be communicated to CT HMIS Lead Agency via the Agency Security Coordinator, consistent the CT HMIS policies and procedures.

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

SECTION 1: CONTRACTUAL REQUIREMENTS AND ROLES **Written: 10/2005**
Revised: 07/2013

POLICY 109: LICENSED END USER **Approved:**

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 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 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.
- 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 **Written: 10/2005**
Revised: 08/2013

POLICY 110: TRAINING SCHEDULE **Approved:**

Policy:

CT HMIS Lead Agency will coordinate training for system users. 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 **Written: 10/2005**
Revised: 07/2013

POLICY 111: AMENDING POLICIES AND PROCEDURES **Approved:**

Policy:

These Policies and Procedures may be amended. It is expected that information will be added, removed and altered as necessary.

Procedure:

Each Continuum has representation on the CT HMIS Steering Committee. 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 making decisions.

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 2:
PARTICIPATION REQUIREMENTS

SECTION 2: PARTICIPATION REQUIREMENTS **Written: 10/2005**
Revised: 07/2013

POLICY 201: PARTICIPATION AND IMPLEMENTATION REQUIREMENTS **Approved:**

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 the CT HMIS Policies and Procedures.

Procedure:

Participating Agencies are responsible for the following responsibilities whether discharged by employed personnel or through contract:

a) 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)
b) Collecting and entering data into CT HMIS as per these policies and procedures
c) Ensuring end users of the program level HMIS compliant system are adhering to the privacy and confidentiality requirements
d) Ensuring end-user participation in trainings
e) Participating in CoC meetings and other initiatives of their CoC(s)
f) Assigning qualified personnel to support initiatives such as the ECM software implementation
g) 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 site visits. Participating Agencies must self-certify that Administrative and Security Checklist requirements are met.

SECTION 2: PARTICIPATION REQUIREMENTS **Written: 10/2005**
Revised: 07/2013

POLICY 202: CT HMIS LEAD AGENCY DATA SECURITY RESPONSIBILITY **Approved:**

Policy:
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.

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;
- 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: 08/2013

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 to have data shared at the level they determine (Attachment). Consumer consent and privacy policies must be followed.

SECTION 2: PARTICIPATION REQUIREMENTS **Written: 10/2005**
Revised: 08/2013
Approved:

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 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 an **oral explanation** and **written consumer consent** for each consumer.

Oral Explanation All consumers will be provided an oral explanation of CT HMIS. The Participating Agency will provide an oral 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 Oral Explanation must contain the following information: (Sample script Attachment)

1. Explanation of CT HMIS:
    - 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:
    - To understand their consumers' needs
    - Help the programs plan to have appropriate resources for the people they serve to inform public policy in an attempt to end homelessness
    - Federal mandate that all HUD funded homeless providers must enter data into an electronic system and capture universal data elements

3. Security
    - Only staff who work directly with consumers or who have administrative responsibilities can look at, enter, or edit consumer records

4. Privacy Protection
    - No information will be released to another agency without written consent
    - Consumer has the right to not answer any question, unless entry into a program requires it
    - Consumer information is transferred in an encrypted format to CT HMIS
    - Consumer has the right to know who has added to, deleted, or edited their CT HMIS electronic record
    - Information that is transferred over the web is through a secure connection

5. Benefits for consumers.
    - Case manager tells consumer what services are offered on site or by referral through the assessment process
    - 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. (Attachment)

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. (Attachment)

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.

SECTION 2: PARTICIPATION REQUIREMENTS **Written: 10/2005**
Revised: 07/2013
POLICY 208: INFORMATION SECURITY PROTOCOLS **Approved:**

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
- Maintain and routinely monitor all system access logs for systems which have access to HMIS data.
- 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 **Written: 07/2013**
Revised:
POLICY 210: Compliance Review **Approved:**

Policy:

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

Procedure:

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 this Agreement that it does not, at the time of execution of this Agreement, meet all requirements for participation in the CT HMIS. Consistent with CT HMIS Policies and Procedures, Agency shall resolve the issues. First time Agency 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 users who are in need of retraining will adhere to the guidelines outlined in the procedure of this policy.

Procedure:
Identification of 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 **Written: 05/2016**
Revised:
POLICY 212: CT HMIS TRAINING NO SHOW POLICY **Approved: 06/2016**

Policy:
CT HMIS trainings are currently provided at no cost to CT HMIS users or potential users. Agencies with new staff, or with existing CT HMIS users who are in need of 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 **Written: 10/2005**

Revised: 07/2013

POLICY 301: MINIMUM REQUIRED DATA ELEMENTS **Approved:**

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:
Link to file page
http://www.cthmis.com/files/file_detail/1919/

Link is also available off of the main conversion page
http://www.cthmis.com/information/info_detail/category/ct_hmis_conversion/

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 **Written: 10/2005**

Revised: 05/2014

POLICY 302: Data Quality Management Plan

Approved:

Policy:

The CT HMIS has a multi-faceted data quality management strategy.
The CT-HMIS Steering Committee Bylaws require a Data Quality Management Subcommittee which is charged with implementing and monitoring the Data Quality Management (DQM) Plan, making recommendations and reporting on a periodic basis. The DQM plan 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 designate an HMIS Data Coordinator (HDC) who is trained on the software and how to run and review program level reports (including data quality). This person is local contact for agency staff and is usually the most knowledgeable person. The HDC is responsible for adherence to the following Data Quality Standards.

Procedure:
The Data Quality Management Plan is based on establishment of and adherence to Data Quality Standards, including the following:

- **Timeliness:**
  Data entry should be current within the scheduled number of days from intake, exit, service provision, or any other client interaction which necessitates any form of data entry. The timeliness schedule is determined by type of program and client contact.

  To ensure data is accessible for agency, community level, and funder reporting as well as to improve data accuracy. Reducing the time period between data collection and data entry will increase the accuracy and completeness of client data. The schedule of timeliness standards will be available on the projects website.

- **Completeness:**
  A current HUD standard of completeness rate, typically 95%, for all CT HMIS participating organizations and HUD funded homeless projects is established and expected.

To ensure that CT HMIS can accurately describe the clients and services provided to clients who are accessing services, a complete and accurate client record is critical for program level reporting, for the use of data in any community level reporting, as well as for HUD required processes such as NOFA and AHAR.

- **Accuracy/Consistency:**
  HDCs are responsible for monitoring the data entry accuracy and consistency of CT HMIS approved data collection tools at their agency level. The CT HMIS Steering Committee and Continuum of Care entities are responsible for approving the data entry collection tools.

  HDCs also monitor the use of the system by approved users, ensuring that users meet the requirements set by their agency, and are appropriately trained in the CT HMIS system and policies before starting access.

  All CT HMIS users must attend training before they are allowed to enter any data into the CT HMIS system. Training includes methods to navigate the system and how to understand the intent of each question asked, to ensure that the data being collected is based on a clear understanding of the question and response options.

  Each Participating Agency must adhere to their own internal policies for conducting logic checks to validate the accuracy of the data in its program-level system and regularly compare data elements to available paper records and updating/correcting missing or inaccurate data. Users must be authorized and trained in order to use the CT HMIS system.

- **Monitoring:**
  The CT HMIS lead organization is responsible for the generation of a monthly statewide report that measures data quality for the previous month. This report focuses on the past month's total active clients, as well as the data quality for those clients. This statewide data quality report is posted on the project website (www.cthmis.com). Agency HDC's are expected to review and make corrections to the data as needed.

  In addition to the data quality report, Continuum and Agency dashboards that highlight both data quality and data completeness are completed on a monthly basis. Data Elements that do not adhere to the CT HMIS Data Quality Standards are highlighted, and the agencies or continuums determine action plans to address concerns. The CoC's are expected to have a data evaluation plan in place.

- **Incentives/Enforcement:**

  The Data Quality Management Committee is charged with the creation, implementation, and maintenance of a Data Quality Management Plan that will recognize and provide positive incentives to outstanding performers, as well as develop corrective action and remediation plans as needed.

RECOGNITION:
Participating Agencies that meet the data quality benchmarks will be periodically recognized by the CT HMIS Steering Committee, and their respective Continuum of Care. CT HMIS participating agencies that do not adhere to the minimum data entry standards set forth herein will be notified of their deficiencies and provided with specific information regarding the nature of the deficiencies and methods by which to correct them.

REMEDIATION ENFORCEMENT:
CT HMIS Data Quality Management Plan will establish a schedule for working with Participating Agencies that are determined to need to correct identified data quality issues. In the corrective action time period, training will be offered to agencies as needed for them to remain compliant with the minimum data entry standards. When there is any progressive discipline for any CT HMIS participating organization, the programs HDC and Director, as well as the CoC leadership and the CT HMIS Steering Committee will all be alerted. CT HMIS participating agencies continuing to perform below the established Data Quality Standards may have their CT HMIS access restricted or suspended, as determined by the CT HMIS Steering Committee, until such time as agencies demonstrate that compliance with minimum data entry standards can be reached.

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 with review and may make the decision follow the recommendations of the Data Quality Management Committee regarding anomalies. The CT HMIS Data Quality Management Committee will conduct continuous quality improvement activities and periodic review of the plan and its implementation, with the oversight of the CT HMIS Steering Committee.

SECTION 4:
USER, LOCATION, PHYSICAL AND DATA ACCESS

SECTION 4: USER, LOCATION, PHYSICAL and DATA ACCESS **Written: 10/2005**
Revised: 07/2013

POLICY 401: ACCESS LEVELS FOR LICENSED END USERS **Approved:**

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 requirements.

SECTION 4: USER, LOCATION, PHYSICAL and DATA ACCESS **Written: 10/2005**
Revised: 07/2013

POLICY 403: ACCESS TO CONSUMER PAPER RECORDS **Approved:**

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 Personal Protect Information (PPI) 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 PPI 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 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 associate with, the date the case note was created, and the reason for the deletion request.