CENTRAL TENNESSEE 503

CONTINUUM OF CARE

Central Tennessee (503)

Homeless Management Information System

Policies and Procedures Manual

Updated July 2020

Table of Contents

1

Key Support Roles & Responsibilities **4**

Central Tennessee 4

Central Tennessee / Designated HMIS Administrator (Pathways MISI) 4

Central Tennessee Continuum of Care (CoC) 5

HMIS Advisory Committee 5

HMIS Partner Agencies 5

HMIS Users 5

HMIS Participation **6**

Mandated 6

Voluntary 6

Minimum Standards to Participate in HMIS 6

HMIS Partnership Termination Policy 7

Initiated by HMIS Partner Agency 7

Initiated by HMIS Lead 7

HMIS Technical Standards **8**

Hardware and Computer Requirements 8

System Availability 9

HMIS Privacy Plan **9**

Data Collection Limitation Policy 9

Client Notification 10

Limitations of HMIS Use 10

Client Rights to Access and Correction of Files 11
Agency's Right to Refuse Inspection of an Individual Record 11
Harassment 11
Data Sharing 12
Protected Agencies and Domestic Violence Agencies 12
HMIS Data Release Policy and Procedures 12
Mandated Reporting 13
Program-Level Data 13
Volunteer Access to HMIS 13

Security Breach Procedures 14
HMIS Data Quality Plan 14
Data Quality Standards and Monitoring 14
Data Collection Requirements 15
Data Quality Training Requirements 15
End-User Initial Training 15
Ongoing Training 15
HMIS Grievance Policy 16
Client Grievance 16
Partner Agency Grievance 16
HMIS Non-Compliance Sanctions 16

Appendix A: Privacy Notice 17
Appendix B: Short Version of Privacy Policy 18
Appendix C: Employee Acknowledgment 19

Key Support Roles & Responsibilities

Franklin Community Development

- Serves as Collaborative Applicant for Central Tennessee Continuum of Care (CoC)
- Ensures fiscal and programmatic compliance with all HUD rules and regulations
- Encourages and facilitates participation

Franklin Community Development
Designated HMIS Administrator

- Serves as HMIS Lead for the Central Tennessee Continuum of Care (CoC) and oversees the daily operation of HMIS
- Ensures the operation of and consistent participation by recipients of funding requiring use of the HMIS system
- Develops written policies and procedures for all HMIS Partner Agencies, which at a minimum includes: a security plan, data quality plan and privacy plan.
- Executes an HMIS participation agreement with each HMIS Partner Agency; this agreement defines performance standards for HMIS system maintenance, training, user support, and reporting/analytical support
- Monitors compliance of all HMIS Partner Agencies
- Ensures that the HMIS Vendor and software is currently in compliance with HMIS standards
- Serves at the primary contact between Partner Agencies and the HMIS vendor
- Serves as the applicant to HUD for grant funds to be used for HMIS Activities for the Continuum of Care's geographic area, as directed by the Continuum, and if selected for an award by HUD, enter into a grant agreement with HUD to carry out the HUD-approved activities

Central Tennessee Continuum of Care (CoC)

- Responsible for selecting one HMIS software system

- Responsible for reviewing, revising, and approving all policy and procedures developed by HMIS Lead; final approval of policies and procedures is the responsibility of the Continuum of Care Board of Directors
- Responsible for implementing all approved and/or revised policies and procedures within six months of approval
- Develops a governance charter and document all assignments and designations consistent with the governance charter.

HMIS Advisory Committee

- Guides the implementation of the HMIS system
- Assists in the development of HMIS policies and procedures in collaboration with the HMIS Lead
- Advises and recommends changes to HMIS policies and procedures for approval by the Planning Committee, General Membership, and Executive Committee of the Central Tennessee CoC
- Examines HMIS aggregate data to offer suggestions on how data measurements can contribute to fulfillment of strategic goals

HMIS Partner Agencies

- Comply with applicable standards set forth by the CoC, HMIS Lead, THDA and HUD, including but not limited to issues of privacy and confidentiality
- Develop agency procedures to ensure and monitor compliance and sanctions for noncompliance
- Ensure staffing and equipment necessary to implement HMIS
- Execute an HMIS Agency Partner Agreement with the HMIS Lead
- Designate an HMIS System Administrator and Chief Privacy Officer

HMIS Users

- Must complete approved training before being given access to HMIS.
- Must read and sign the CoC’s HMIS Users Agreement acknowledging acceptance of the privacy/ security requirements of the Privacy Notice
- Must complete annual training requirements of the Continuum
- Responsible for the accuracy of client information entered in HMIS; Missing data rates are expected to be below 5%

- Responsible for entering client data in a timely manner; within 72 hours of project entry and within 72 hours of project exit

HMIS Participation

Mandated

Agencies receiving Emergency Shelter Grants, Continuum of Care grants, Shelter plus Care grants, Section 8 SRO programs, HOPWA, SSVF grants and other funders within the Continuum of Care will be required to meet the minimum HMIS participation standards. Participating agencies must agree to execute and comply with an HMIS Agency Partner Agreement, as well as all HMIS policies and procedures.

Voluntary

While the Central Tennessee CoC does not require participation in HMIS by agencies that do not receive HUD CoC or Emergency Solutions Grant funding, every effort is made to encourage all homeless service providers to participate in the HMIS system in order to gain a more thorough understanding of the needs of those experiencing homelessness in Central Tennessee.

Minimum Standards to Participate in HMIS

- Partner Agencies will enter into an HMIS Agency Partner Agreement and comply with all HUD regulations for HMIS participation
- Partner Agencies will designate a Chief Privacy Officer. The Chief Privacy Officer is responsible for: managing client questions and complaints about the Privacy Notice, ensuring all new users have completed a User Agreement, monitoring all users compliance with training requirements, and maintaining both user and technological requirements needed for security standards.
- All users are responsible for collecting all Universal Data elements (UDE) and Program-Specific data elements (PD) as appropriate based on project funding.

In addition, additional data elements may be required by the Central Tennessee CoC

- All users must enter client-level data into the HMIS system within 72 hours of entry into a project and within 72 hours of exit from a project.
- All users are required to participate in HMIS training annually to stay abreast of all HMIS requirements and software updates. The HMIS Lead and HMIS Agency Administrator will communicate training opportunities to users.

HMIS Partnership Termination Policy

Initiated by HMIS Partner Agency

Contributing HMIS Organizations may terminate the HMIS Partner Agreement with or without cause upon 30 days written notice to the HMIS Lead and according to the terms specified in the HMIS Partner Agreement. The termination of the HMIS Partner Agreement by the Partner Agency may impact compliance with other agreements and regulations, such as contracts with the Tennessee Housing Development Agency (THDA) that specify HMIS utilization. In the event of termination of the HMIS Partner Agreement, all data entered into the HMIS system will remain active, and records will remain open or closed according to any data sharing agreements in place at the time of termination. In all cases of termination of HMIS Partner Agreements, the HMIS Administrator will inactivate all users from that agency on the date of termination of agreement. The HMIS Administrator will notify the HMIS Advisory Committee and the HMIS Lead when these tasks are completed.

Initiated by HMIS Lead

The HMIS Lead may terminate the HMIS Partner Agreement for noncompliance within the terms of that contract upon 30 days written notice to the HMIS Partner Agency. The HMIS Lead will require any violations to be rectified to avoid termination of the HMIS Partner Agreement.

The HMIS Lead may also terminate the HMIS Partner Agreement with or without cause upon 30 days' written notice to the HMIS Partner Agreement and according to the terms specified in the HMIS Partner Agreement.

The termination of the HMIS Partner Agreement may impact other compliance regulations; such as contracts with the Department of Human Services that specify HMIS utilization. In

the event of termination of the HMIS Agency Agreement, all data entered into the HMIS system will be maintained by the HMIS Lead until all clients are appropriately exited from the terminated agency.

HMIS Technical Standards

The HMIS Lead and HMIS vendor are equally responsible for compliance with any and all technical standards issued by HUD. HUD has established that all HMIS software must be able to: produce unduplicated client records, collect all data elements set forth by HUD, report outputs, produce compliance reports for Partner Agencies and the Lead to assess achievements with established benchmarks, and generate standardized audit reports.

Hardware and Computer Requirements

While the HMIS Lead and HMIS vendor are responsible for supplying software that meets HUD standards, Partner Agencies are responsible for complying with agency-level system security standards. These system standards aid in the safety and integrity of client records. Partner Agencies must comply with the following hardware and software standards:

- Secure broadband internet must be used; Wi-Fi is acceptable if the connection is protected by a network security code
- Computers must have an operating system compatible with the current HMIS software
- Computers must have an Internet browser compatible with current HMIS software
- All workstations must be protected with a screensaver that engages automatically if a user leaves the workstation when HMIS software is active ● All workstations must have current and active security which include:
    a. Real-time antivirus scanning
    b. Automatic virus removal
    c. Anti-Spyware
    d. Firewall
    e. Anti-phishing protection

The equipment used to connect to the HMIS system is the responsibility of the HMIS Partner Agency. Contributing HMIS Partner Agencies will need to provide their own internal

technical support for the hardware, software and Internet connections necessary to connect to the HMIS system.

System Availability

It is the intent of the HMIS Lead and HMIS Vendor that the HMIS system server will be available 24 hours a day, 7 days a week, and 52 weeks a year to incoming connections. However, no computer system achieves 100 percent uptime. In the event of planned server downtime, the HMIS Lead will inform agencies as much in advance as possible in order to allow HMIS Partner Agencies to plan their access patterns accordingly. Annual reviews for Technical Standard Compliance will be conducted by each Partner
Agency Chief Privacy Officer to ensure agencies are meeting requirements. The HMIS Lead will also conduct technical standards audits on behalf of the entire CoC to ensure Partner Agencies and HMIS system software are in compliance with applicable standards.

HMIS Privacy Plan

Data Collection Limitation Policy

Partner agencies will only enter client information into the HMIS system that is deemed necessary to provide quality service. Partner agencies, in collaboration with the CHP, the HMIS Administrator, will make a determination of what qualifies as essential for services. Partner agencies reserve the right to decline services to clients refusing to share information necessary to verify program eligibility as doing so could jeopardize the agency’s status as a service provider. The agency assumes clients requesting services will agree to provide required information and commit to using or disclosing the information as described in the privacy notice or as allowed/required by law.

Client Notification

Partner Agencies must post notification advising clients of the Privacy Notice (Appendix A) at each intake desk of the agency. Clients must also be provided with the short version of the Privacy Notice (Appendix B) which advises them that they can request a copy of the full policy.

The HMIS Privacy Notice should be posted on each Partner Agency's web page. Agencies should ensure that the address does not appear in the Privacy Notice before it is posted on their website, if the address is not public knowledge.

In addition to the posted notification signs, any client who agrees to allow HMIS User access to their HMIS profile must sign a Client Authorization form. This form must be updated annually.

The agency must provide reasonable accommodations for persons with disabilities throughout the data collection process. Various versions of the Privacy Notice will be made available through the HMIS Lead.

Limitations of HMIS Use

Partner agencies will use and disclose personal information from HMIS only in the following circumstances:

- To provide or coordinate services to an individual
- For functions related to payment or reimbursement for services
- To carry out administrative functions including, but not limited to legal, audit, personnel, planning, oversight or management functions.
- Databases used for research, where identifying information has been removed.
- Contractual research where privacy conditions are met.
- Where a disclosure is required by law and disclosure complies with and is limited to the requirements of the law. Instances where this might occur are during a medical

emergency, to report a crime against staff of the agency or a crime on agency premises, or to avert a serious threat to health or safety, including a person's attempt to harm himself or herself.
- To comply with government reporting obligations.
- In connection with a court order, warrant or other court proceeding requiring disclosure.

Client Rights to Access and Correction of Files

Any client receiving services from a Partner Agency has the following rights:

- Access to program records. Clients have the right to review their records in a program in the HMIS. A written request should be made to the HMIS Agency Administrator, who should follow-up on the request within five working days.
- Access to full records. Clients have the right to review their full record in the HMIS. They may make a written request through the HMIS Agency Administrator, who must request approval from the HMIS Lead within five working days.
- Correction of an HMIS record. A client has the right to request that his or her HMIS record is correct so that information is accurate. This ensures fairness in its use.
- Refusal. A client has a right to refuse to participate in HMIS or to provide personal information. The agency's ability to assist a client depends on the documentation of certain personal identifying information, and may decline to provide services to a client who refuses to provide this data.

Agency's Right to Refuse Inspection of an Individual Record

The Partner Agency may deny a client the right to inspect or copy his or her personal information for the following reasons:

- information is compiled in reasonable anticipation of litigation or comparable proceedings;
- information about another individual other than the Partner Agency staff would be disclosed;
- information was obtained under a promise of confidentiality other than a promise from the provider and disclosure would reveal the source of the information; or
- Information reasonably likely to endanger the life or physical safety of any individual if disclosed.

Harassment

The agency reserves the right to reject repeated or harassing requests for access or correction. However, if the agency denies a client's request for access or correction, written documentation regarding the request and the reason for denial will be provided to the client. A copy of that documentation will also be included in the client record.

Data Sharing

At initial project intake, the client should receive a verbal explanation and written documentation about utilization of the HMIS system for Central Tennessee Continuum of Care. If a client is willing to share information with HMIS, they must sign a Client Authorization form. Any information that will be shared, beyond what is covered by the Client Authorization for HMIS, will require additional written consents and release of information by the client.

The client does have the right to revoke written authorization at any time, unless this is overridden by agency policy or is a part of a conditional agreement with the provider. Once the client has revoked their authorization, no new information may be utilized in HMIS but all historical data remains accessible by the provider.

All Partner Agencies are expected to uphold federal, state, and local confidentiality regulations to protect records and privacy. If an agency is covered by the Health Insurance Portability and Accountability Act (HIPAA), the HIPAA\HITECH regulations prevail.

Protected Agencies and Domestic Violence Agencies

Protected agencies serve populations that require special security and privacy considerations. Populations include medically fragile, at-risk youth, and those served by Shelter+Care programs. Protected agencies contribute data to HMIS; however, information about clients receiving services is restricted. Only individuals with specific privileges can access the information.

Domestic violence agencies are prohibited from entering data into the HMIS. If domestic violence agencies receive CoC or ESG funding, they are required to have an HMIS-comparable database, and the HMIS lead will work with agencies to ensure the databases

they select meet HUD standards. These agencies are required to report aggregate data for reporting purposes.

HMIS Data Release Policy and Procedures

HMIS Users may access client-level data for their specified project(s) only after obtaining and documenting appropriate client authorization. **Client authorization is good for up to 1 year**. After one year, only historical record information will be available for the project unless an updated client authorization is filed.

Client-level data may also be viewed by only the HMIS Lead and HMIS Vendor for purposes of compliance, software correction, data quality issues resolution, and other required tasks related to HMIS privacy, security, and data quality standards.

No identifiable client data are to be released to any person, agency or organization without written consent by the client, unless otherwise required by law.

Mandated Reporting

Mandatory reporters should comply with state guidelines for reporters. This obligation supersedes any agency policies that prohibit disclosure of identifying information.

Program-Level Data

The HMIS Lead will supply the HMIS Committee quarterly reports analyzing program-level aggregate data. The reports will help guide the creation of systematic practice for the Continuum of Care. At a minimum, the HMIS Advisory Committee will report findings and offer practice suggestions to the COC Board of Directors at least twice a year.

Agencies will be able to request access to aggregate-level data. The HMIS Agency Administrator will make requests through the HMIS Lead, who will outline appropriate use and dissemination of aggregated data. Training and support will be made available through the HMIS Lead. Public release of community-wide statements based on aggregate data requests must be coordinated through the CoC. No individually identifiable client data will be reported in any of these reports.

Volunteer Access to HMIS

Volunteers may have limited access to HMIS and client service records. (A volunteer is an individual who provides assistance to an agency in limited capacity, and without the benefit of a pre-screening

or background check) Volunteers may view or edit basic demographic information about clients (the profile screen), but are restricted from all other screens in HMIS. A volunteer may also enter new clients, make referrals, and check clients in/out from a shelter. A volunteer does not have access to the “Services Provided” tab. This access level is designed to allow a volunteer to perform basic intake steps with a new client and then refer the client to an agency staff member or case manager for work that requires access to more sensitive client information.

Security Breach Procedures

A security breach includes, but is not limited to, unauthorized sharing of username and passwords information, and emailing Personally Identifying Information (PII). Both actions are cause for serious concern and could potentially jeopardize client confidentiality. If a security breach is confirmed, the following protocol outlines the process the HMIS Administrator will use to respond to HMIS security breaches.

- Inactivate affected user accounts immediately.
- Notify the user’s or users’ supervisor(s) and Executive Director or equivalent.
- Notify the HMIS Lead
- Investigate circumstances surrounding breach

User access may be reactivated at HMIS Lead Agency’s discretion, but the user(s) must take and pass the Privacy and Security test before they can regain access to the HMIS.

HMIS Data Quality Plan

It is ultimately the responsibility of the Central Tennessee Continuum of Care Board of Directors and HMIS Lead to ensure quality data is submitted to HUD. The HMIS Administrator will work closely with the HMIS Lead and the staff of all participating agencies to verify the accuracy, timeliness and completeness of HMIS data on a monthly basis. In addition, the CoC HMIS Committee will receive quarterly reviews of agency level data quality. This information will be used to identify potential training needs, gaps in HMIS participation and continuum-wide improvement suggestions. Program-level data quality may also be used for system analysis and evaluations.

Data Quality Standards and Monitoring

- Accuracy: All data entered will be accurate. Any patterns of errors identified by users will be reported to the HMIS Administrator. When patterns of error have been discovered, users will be required to correct the data, modify data entry processes (if applicable) and will be monitored for compliance.
- Completeness: entries of “client does not know”, “client refused” or “data not collected” in required data fields will not exceed 5 percent required for CoC reporting. Per HUD data

standards, blank entries in required data fields are not allowed. Project level reporting must indicate all participants meet the appropriate eligibility requirements (ie., homeless at entry, has a disabling condition, etc)

- Timeliness: universal data elements (at a minimum) must be entered into the HMIS system within 72 hours of entry into a project and complete appropriate discharge within 72 hours of exit from a project.

HMIS Administrators will ensure compliance with Data Quality Standards by performing monthly data quality checks in accordance with the Data Quality Plan.

Data Collection Requirements

Partner Agencies are responsible for completing, at minimum, the HUD defined Universal Data Elements (UDE's) and any HUD Program-specific Data Elements required for the agency's project. Partner Agencies may also be required to collect data elements determined by the HMIS Committee to be vital. Partner Agencies will do their due diligence to collect and verify client information upon client initial program enrollment or as soon as possible. Any information collected by a Partner Agency must be documented in HMIS within 72 hours of entry into a project and appropriate discharges must be completed within 72 hours of exit from a project.

Data Quality Training Requirements

In order for the HMIS system to be a benefit to clients, a tool for Partner Agencies and a guide for planners, all users must be adequately trained to collect, enter, and extract data. The HMIS Administrator will be responsible for developing an annual training schedule. The annual training schedule must include various types and levels of training- for beginning users and advanced users. Trainings can be offered either in person or through online webinars.

End-User Initial Training

All HMIS Users must complete approved training before being given access to HMIS. Users should be trained on: use of HMIS software and the confidentiality/security requirements of the Privacy Notice. As part of the training, each employee and volunteer of your agency who collects, reads, or is otherwise exposed to client information must be given a copy of the full Privacy Notice, be allowed to read it, then must sign the Acknowledgment enclosed in this manual as Appendix C to confirm they have read and understood the policy.
It is encouraged that all HMIS Users also receive agency-specific training in order to fulfill Partner Agency expectations for entering data.

Ongoing Training

In order to remain current on HUD standards and local continuum expectations, all HMIS users are required to complete annual training and training on all HMIS software updates. These ongoing trainings can be in the form of: attendance at User Group meetings, participation in approved online/in-person trainings, and individualized meetings with HMIS Administrators. The HMIS Lead will communicate training opportunities to users.

Documentation of training will be made available by the HMIS Administrator. It is the expectation that the Agency Chief Privacy Officer will maintain a record of each HMIS User's completed training hours for one year. Training records should be submitted in the annual compliance review.

HMIS Grievance Policy

Client Grievance

Clients have the right to be heard if they feel that their confidentiality rights have been violated, if they have been denied access to their personal records, or if they have been put at personal risk or harmed. Each agency must establish a formal grievance process for the client to use in such a circumstance. To file an HMIS related complaint or grievance they should contact the agency's Chief Privacy Officer. HMIS Partner Agencies will report all HMIS related client grievances to the HMIS Administrator. The Administrator will record all grievances and report any common trends in complaints to the HMIS Lead and the HMIS Advisory Committee.

Partner Agency Grievance

It is encouraged that if any issues arise, problems should be presented and resolved at the lowest possible level. If HMIS users have an issue with HMIS software or policy, they should reach out to the HMIS Administrator. If an issue cannot be successfully resolved, the HMIS Lead will be notified.

HMIS Non-Compliance Sanctions

The HMIS Lead is responsible for establishing appropriate sanctions for non-compliance issues. These sanctions must be approved by the Central Tennessee Continuum of Care, and may include suspension of HMIS system access. Additionally, HMIS Partner Agencies must also have agency-specific sanctions for users not in compliance with HMIS policies and procedures.

Appendix A: Privacy Notice

Notice to Public

We collect personal information directly from you for reasons that are discussed in our privacy statement. Our primary focus is to understand your needs. We may be required to collect some personal information by law or by organizations that provide funding to operate this program. Other personal information that we collect is important to run our programs, to improve the quality of services we offer, and to better coordinate services on your behalf. We only collect information that we consider to be appropriate. You may request a copy of our full Privacy Notice.

Appendix B: Short Version of Privacy Policy

Homeless Management Information System
Summary of Privacy Notice

Introduction. HMIS is a computer system for data collection that was created to meet a requirement for the United States Congress. This requirement was passed in order to get a more accurate count for individuals and families who are homeless and to identify the need for various services. Many agencies use this system and share information.

Information in the HMIS System about you that we may share includes:

1) Basic identifying demographic data (name, address, phone number, date of birth).
2) The nature of your situation.
3) Services and referrals you receive from our agency.

Our ability to assist you depends on having certain personal identifying information. If you choose not to share information we request, we could potentially decline to provide you services as doing so could jeopardize our status as a service provider. We assume that, by requesting services from our agency, you agree to allow us to collect information and to use or disclose it as described in this notice and otherwise as allowed or required by law.

Your personal data will be used only by this agency or others to which you are referred for services.

Confidentiality Rights: Maintaining the privacy and safety of those using our services is very important to us. This agency follows all confidentiality regulations and also has its own confidentiality policy.

Your Information Rights: As a client, you have the following rights:

1. Access to your record at your request.
2. Request a correction of your record.
3. File a grievance if you feel that you have been unjustly served, put at personal risk, harmed, or your personal information was not handled correctly.

When Information Is Disclosed: The full Privacy Notice sets forth situations when your personal information might be disclosed.

Benefits of HMIS and Agency Information Sharing: Allowing us to share your real name results in a more accurate count of individuals and services used. A more accurate count is important because it can help us and other agencies to meet the needs of our clients, such as:

1. Better identify / coordinate need for services / to demonstrate assistance needed in our area.
2. Obtain additional funding and resources to provide services.
3. Plan and deliver quality services to you and your family.
4. Assist the agency to improve its work.
5. Keep required statistics for state and federal funders.
6. Promote coordination of services so your needs are better met.
7. Make referrals easier by reducing paperwork.
8. Avoid having to report as much information to get assistance from other agencies.

You may keep this summary of the policy. A copy of the full privacy notice is available upon request.

Appendix C: Member Acknowledgment

_____

Agency Name

Member Acknowledgment of Privacy Notice

I, _____, hereby acknowledge that I have received, read and pledge to comply with the Homeless Management Information System Privacy Notice.

_____ _____

Date Name