



Knoxville Homeless Management Information System

(865) 974-9142

hmissupport@utk.edu

www.KnoxHMIS.org

HMIS Policies & Procedures Manual (Version 5)

KnoxHMIS Project Policies & Procedures

Purpose

This document provides the policies, procedures, guidelines, and standards that govern the Knoxville-Knox County Continuum of Care Homeless Management Information System (KnoxHMIS) agencies contributing data (HMIS Partnering Agencies) to the KnoxHMIS. HMIS staff will provide each HMIS Member Agency providers with a copy of this document. As a condition of participation, each HMIS Member Agency is asked to adhere to all policies within the document as signed in the HMIS Memorandum of Understanding (MOU).

Exceptions

In order to mitigate risk from participation in the HMIS system, HMIS leadership has the right to grant exemptions to any HMIS policy only in the following instances:

1. Unique circumstances/projects not encountered before by HMIS staff,
2. Public policy decisions needing some considerations,
3. On need of quick time lines for implementation.

No other instances will be considered.

Acknowledgments

The KnoxHMIS staff would like to thank its many statewide and national colleagues who have shared their policies with us, while in development of this document. We would also like to thank the HMIS Member Agencies for their thoughts, ideas, and work to help draft and revise this document.

Table of Contents

Section 1: Historical Perspective

Introduction	05
HMIS Project Goals	06
Measure the Extent and Nature of Homelessness	06
Streamline the Intake and Referral Process for Human Service Agencies	06
Provision for In-depth Case Management by Sharing Client Information	06
Inventory Homeless Housing	06

Section 2: HMIS Roles & Responsibilities

Roles	07
Responsibilities	07
Annual Projects	08

Section 3: HMIS Member Agency Roles & Responsibilities

Member Agency Role & Responsibilities	10
Participation Requirements	10
HMIS Member Agency Agreement	10
HIPAA Agreement	11
Roles and Requirements	11
Minimal Technical Requirements	14
HMIS Data Use	15
HMIS Corrective Action	16
Potential Courses of Action	17

Section 4: User Administration

HMIS End User Prerequisites	19
HMIS End User Agreement	19
License Administration	20
Law Enforcement	22

Section 5: Clients Rights

Client Consent & Release of Information	23
Filing a Grievance	24
Revoking Authorization for HMIS Data Collection	25

Section 6: Privacy, Safety & Security

National Privacy Requirements	26
Privacy Notice	26
System Security and Privacy Statement	27
Data Ownership	29

Section 7: User Training	
HMIS Training Process	30
Section 8: HMIS Technical Support	
Technical Support	31
Section 9: Data Collection Process	
Clients Served vs. Clients Benefiting from Service	33
Data Entry Requirements	33
Managing Bed Inventory (Housing Providers Only)	35
Optional Requirements	35
Client Self-Sufficiency Outcomes Matrix	35
HMIS Client Photo ID Cards	36
Section 10: Data Quality	
Data Quality	37
Section 11: Performance Measurement	
Performance Measures	42
Signature Page	43
Appendix: Glossary	
HUD & HMIS Acronyms & Definitions	44
HMIS Service Point Data Dictionary	52
HMIS Reports	59
HUD & Partners' Acronyms	60
Homelessness Definitions	62

Section 1: Historical Perspective

Introduction

The concept of HMIS was a brainchild of the United States Congress and the Department of Housing and Urban Development (HUD). In 1999, Congress mandated the Department of Housing and Urban Development (HUD) find a way to adequately track the scope of homelessness in the United States in the HUD Appropriations Act. The following year, the Department of Housing and Urban Development (HUD) mandated that each community implement or be in the process of implementation of a Homeless Management Information System (HMIS) by October 2004.

HMIS is a secure web-based centralized database where non-profit organizations across our community enter, manage, share, and report information about the clients that they serve. The HMIS staff provides training and technical assistance to HMIS Member Agency providers and their users.

Senate and House Appropriations Committee reports have reiterated Congress' directive to HUD to: 1) assist communities in implementing local Homeless Management Information Systems (HMIS), and 2) develop an Annual Homeless Assessment Report (AHAR) that is based on HMIS data from a representative sample of communities. Most recently, Congress renewed its support for the HMIS initiative and the AHAR in conjunction with the passage of the Transportation, Treasury, Housing and Urban Development, the Judiciary, the District of Columbia, and Independent Agencies Appropriations Act of 2006 (PL 109-115).

In addition to Congressional direction HUD, other federal agencies and the U.S. Inter-agency Council on Homelessness requires HMIS under various statutory authorities and Congressional direction to collect information about the nature and extent of homelessness. Individual projects authorized under the McKinney-Vento Act require the assessment of homeless needs, the provision of services to address those needs, and reporting on the outcomes of federal assistance in helping homeless people to become more independent. The major congressional imperatives in HUD's McKinney-Vento Act projects are:

- Assessing the service needs of homeless persons;
- Ensuring that services are directed to meeting those needs;
- Assessing the outcomes of these services in enabling homeless persons to become more self-sufficient; and
- Reporting to Congress on the characteristics of homeless persons and effectiveness of federal efforts to address homelessness.

HMIS Project Goals

Measure the Extent and Nature of Homelessness

The first goal is to inform public policy makers about the extent and nature of the homeless population in our community. This is accomplished through analysis of homeless client and service provider data. HMIS gathers an unduplicated count of those accessing services, service trends, bed utilization rates, re-entry rates, and HMIS system usage. All data is provided in an aggregated (void of any identifying client level information) format and made available to public policy makers, service providers, advocates, and consumer representatives.

Streamline the Intake and Referral Process for Human Service Agencies

The second goal is to streamline the intake and referral process for human service agencies in the community. HMIS provides a standardized mechanism for collecting client information across all providers. Human service providers collect the same client information and then the client can share that information at each project with additional service providers for greater ease of service. As part of the system, a service provider can send an electronic referral to another agency. This streamlined process allows for the development of centralized coordinated assessment centers where agencies can store assessments, refer to other projects, and follow clients longitudinally with a shared information system.

Provision for In-depth Case Management by Sharing Client Information

The third goal is to allow for in-depth case management through the sharing of client information in a centralized system. HMIS provides a standardized mechanism in which human service providers collect information and then share it among every participating human service agency to assist clients more efficiently and effectively.

Inventory Homeless Housing

Finally, the fourth goal is to inventory homeless housing options in the community. HMIS captures this inventory and allows for real-time collection and tracking of emergency shelter, transitional housing, and permanent supportive housing.

Section 2: HMIS Roles & Responsibilities

Roles

(HMIS) is to act as the Homeless Management Information System (HMIS) Lead Agency for the community.

In addition to acting as the HMIS Lead Agency, the role of HMIS is to provide training and technical support to HMIS Member Agency providers. Lastly, HMIS staff coordinates and participates in numerous projects annually regarding data collection and performance measurement.

Responsibilities

HMIS Staff is responsible for coordinating the following items on behalf of HMIS Member Agencies:

- **All software related issues to the software vendor** - This includes all communication with the vendor including phone, email, and conferences as well as submitting feature enhancement requests from HMIS Member Agencies.
- **User training** - HMIS staff is responsible for all End User training. This is to ensure continuity and consistency with training as well as to ensure the proper workflow for HMIS Member Agencies.
- **Technical support as it relates to the software or project** - HMIS staff is responsible for providing technical support to Agency Administrators and End Users. Technical support services attempt to help the user solve specific problems with a product and do not include in-depth training, customization, reporting, or other support services.
- **Data quality initiatives** – Together, Member Agencies and HMIS staff work diligently on adhering to data quality standards in order to ensure that reports both at the provider level and the system level are complete, consistent, accurate, and timely.
- **System-wide reporting on performance measures for local, state and national initiatives** - HMIS staff train HMIS Member Agencies on how to access and run reports on the data they contribute to the HMIS. Additionally, reports are provided to local community planners monthly and to statewide and national partners quarterly and annually. These data are in an aggregate format and details the trends on how clients are being served in the community.

Annual Projects & Reports

HMIS Staff coordinates and/or participates in numerous projects annually that include, but are not limited to, data collection and reporting. Below is a list of current HMIS projects:

- **Annual Homeless Assessment Report (AHAR)** -The Annual Homeless Assessment Report (AHAR) is a report submitted to the Department of Housing and Urban Development (HUD). Data are then submitted to the U.S. Congress detailing the extent and nature of homelessness in the United States. It provides counts of the homeless population and describes their demographic characteristics and service use patterns. The AHAR is based primarily on data from the Homeless Management Information System (HMIS) in the United States.
- **Annual Performance Report (APR)** - The Annual Progress Report (APR) provides annual performance reporting on clients' outputs and outcomes that enables an assessment of grantee performance in achieving the housing stability outcome measure. The APR fulfills statutory reporting requirements and provides the grantee and HUD with the necessary information to assess the overall performance and accomplishment of the grantee's program activities under the approved goals and objectives.
- **Grant Inventory Worksheet (GIW)** – The Grant Inventory Worksheet (GIW) provides CoCs and Department of Housing and Urban Development (HUD) Field Offices with information about CoC program grants that are eligible for renewal in the FYXXXX competition.
- **HOPWA Consolidated Annual Performance and Evaluation Report (CAPER)** - The CAPER report for HOPWA formula grantees provides annual information on program accomplishments that supports program evaluation and the ability to measure program beneficiary outcomes as related to: maintain housing stability; prevent homelessness; and improve access to care and support.
- **Housing Inventory Chart (HIC)** - The Housing Inventory Chart (HIC) is an annual report submitted to the Department of Housing and Urban Development (HUD) that lists all homeless emergency, transitional, safe haven, shelter plus care, and permanent supportive housing beds in our Continuum of Care (CoC).
- **Homeless Point in Time (PIT)** - Bi-annually our Continuum of Care (CoC) is responsible for counting and surveying the homeless population on a given day and submitting those data to local, state and federal government entities. These data are used to estimate the number of individuals in our community experiencing homelessness.
- **System Performance Measures (SPMs)**-- The System Performance Measures (SPM) is a report submitted to the Department of Housing and Urban Development (HUD) annually for the report period of October 1—September 30. Data submitted to HUD review data entered throughout the HMIS by all HMIS partners regardless of funding streams. Metrics included in the report include: length of time persons remain homeless, Extent to which Persons who Exit Homelessness Return to Homelessness, Number of Homeless Persons, Employment and Income Growth for Homeless Persons in CoC Program-funded Projects, Number of Persons who Become Homeless for the First Time, Homelessness Prevention and Housing Placement, and Successful Housing Placements.

Section 3: HMIS Member Agency Roles & Responsibilities

"HMIS Member Agency" is the term given by the HMIS staff to reference participating health care and/or human service providers who actively enter data into the HMIS.

Participation Requirements

Policy 3.1: A qualified HMIS Member Agency is required to sign and abide by the terms of the HMIS Member Agency Agreement, the HMIS HIPAA Agreement, and the HMIS Policies and Procedures.

Procedure: Any organization that provides a health and human service may qualify to participate in HMIS. To participate in HMIS, Member Agencies must sign and agree to abide by the terms of the HMIS Member Agency Agreement and the HMIS HIPAA Agreement. They must also abide by the policies and procedures outlined in this document as well as the End User Agreement. All Member Agencies which receive funding from the United States Housing and Urban Development Department (HUD) are mandated to participate in HMIS by contract. For other agencies, participation is voluntary and strongly encouraged by the local CoC.

HMIS Member Agency Agreement

Policy 3.2: The HMIS Member Agency Agreement must be signed by an authorized representative of each HMIS Member Agency.

Document: The HMIS Member Agency Agreement is a legal contract between the HMIS Member Agency and the HMIS Lead Agency regarding specific HMIS guidelines and use. The agreement outlines specific details about the HMIS Member Agency providers' HMIS involvement including, but not limited to, the areas of confidentiality, data entry, security, data quality and reporting.

Procedure for Execution:

1. The Agency's Executive Director (or authorized officer) will sign two copies of the HMIS Member Agency Agreement and mail them to the HMIS Lead Agency.
2. Upon receipt of the signed agreement, it will be signed by the HMIS Lead Agency director.

3. One copy of the HMIS Member Agency Agreement will be scanned and filed, both as a hard copy and electronically with the HMIS Lead Agency. The original copy will be mailed back to the HMIS Member Agency.

HIPAA Agreement

Policy 3.3: The HIPAA Agreement must be signed by the Executive Director (or authorized representative) of each HMIS Member Agency.

Procedure: The HIPAA Agreement is an HMIS document required by all HMIS Member Agency providers who partner with HMIS. This document details the basic business practices of the HIPAA rules to be followed by each HMIS Member Agency. The document further explains that each HMIS Member Agency will be working with other HMIS Member Agency providers who are HIPAA covered entities. All HMIS End Users will adhere to the basic business practices under HIPAA as it relates to client confidentiality, privacy, and security.

1. The Agency's Executive Director (or authorized officer) will sign two copies of the HMIS HIPAA Agreement and mail them to the HMIS Lead Agency.
2. Upon receipt of the signed agreement, it will be signed by the HMIS Lead Agency director.
3. One copy of the HMIS HIPAA Agreement will be scanned and filed, both as a hard copy and electronically with the HMIS Lead Agency. The original copy will be mailed back to the HMIS Member Agency.

Agency Staff Roles and Requirements

Policy 3.4: For a Member Agency with more than five employees and licensed end users, the Member Agency will assign both an Agency Administrator and a back-up Agency Administrator to coordinate HMIS activities for their organization.

Procedure: The Executive Director (or authorized officer) of the Agency will complete the Agency Administrator Designation Form to assign the position to a specific staff person. This role is vital to the success of HMIS at the HMIS Member Agency locations. This practice will ensure that the data is entered in a timely manner, the quality of the data is continuously monitored, and communication and support between HMIS and the HMIS Member Agency is streamlined. An Agency Administrator is the staff member at an HMIS Member Agency provider who acts as the centralized contact for the HMIS staff.

Agency Administrator Role and Responsibility

The Agency Administrator role is to act as the operating manager and liaison for the HMIS system at the HMIS Member Agency. This position is required for any Member Agency with five or more active licenses.

They are responsible for the following items:

- Adhere to and enforce the HMIS Policies and Procedures.
- Attend at least one Agency Administrator Training.
- Maintain current user license in the system by completing the certification assignments within 5 days of training and login to the system at least once every 30 days.
- Communicate and authorize personnel and security changes for HMIS End Users to HMIS Staff within 24 hours of a change.
- Act as the first tier of support for HMIS End Users.
- Ensure client privacy, security, and confidentiality for clients.
- Enforce HMIS End User Agreements.
- Ensure the HMIS Privacy Notice is posted in a visible area of the Agency and communicated in a language understandable by clients.
- Enforce data collection, entry, and quality standards.
- Ensure a basic competency with running HMIS system reports and have an understanding of system wide data quality reports.
- Ensure Agency and all users are using the correct HMIS related forms and following the most current HMIS procedures and work flow.
- Attend all HMIS required meetings and conference calls.
- Assist with HMIS projects as needed (AHAR, PIT, EHIC, and Pulse).
- Schedule/Authorize HMIS End User Training.
- Inform HMIS Staff of all project changes within at least five business days prior to the change.

Policy 3.4.1: For Member Agencies with less than five employees and licensed end users, an Agency Administrator is not required, but at least one HMIS Point of Contact is required to communicate with the HMIS staff.

Point of Contact Role and Responsibility

The Point of Contact role is very similar to the Agency Administrator role, but without the technical support aspect. The HMIS staff will fulfill the role of help desk support and triage. A Member Agency should designate a primary and a back-up Point of Contact. The HMIS Point of Contact is responsible for the following items:

- Adhere to and enforce the HMIS Policies and Procedures.
- Enforce HMIS User Agreements.
- Ensure client privacy, security, and confidentiality.
- Communicate and authorize personnel/security changes for HMIS End Users to HMIS Staff within 24 hours of a change.
- Authorize HMIS End Users by completing the HMIS End User Request Form prior to trainings.
- Ensure Agency and all users are using the correct HMIS related forms and following the most current HMIS work flow.
- Inform HMIS Staff of all project changes with at least five business days prior to the change.
- Ensure the HMIS Privacy Notice is posted in a visible area of the Agency and communicated in a language understandable by clients.
- Attend all HMIS required meetings and conference calls.
- Assist with HMIS projects as needed (AHAR, PIT, eHIC, and Pulse).

Policy 3.5: A HMIS Member Agency will ensure that at least one person will complete training in order to receive a license to access live client data in HMIS.

Procedure: Once the Agency Administrator/Point of Contact position has been assigned, he or she will be able to work with HMIS Staff to assign End Users and authorize additional licenses for the HMIS Member Agency. The End User will complete training and then be responsible for the timeliness of the data being entered and the quality of the data they enter.

An **End User** is a term used to refer to all HMIS users at an HMIS Member Agency.

HMIS End Users Roles and Responsibility

Every HMIS End User must attend at least one training session and sign an HMIS End User Agreement. This should be completed within five business days of training.

Every HMIS End User is responsible for the following items:

- Adhering to all of the Policy and Procedures outlined in this document.
- Attending all trainings required by HMIS staff and the HMIS Member Agency Administrator.
- Entering quality data in a timely and accurate manner.

- Adhere to the data requirements set by the HMIS staff and the HMIS Member Agency.

Initial HMIS Staff Site Visit

Policy 3.6: Prior to signing the HMIS agreements, a prospective HMIS Member Agency will first schedule and complete an on-site Initial HMIS Site Visit at the prospective Member Agency.

Procedure: Prior to signing the Agreements for participation, a prospective HMIS Member Agency provider will first schedule and complete an on-site Initial HMIS site visit at the prospective Member Agency. This site visit is between the HMIS staff, the prospective HMIS Member Agency Executive Director, and other HMIS Member Agency critical staff at the prospective HMIS Member Agency location. Other staff may include data entry staff, supervisors, managers, intake workers, or case managers. The prospective HMIS Member Agency should include any staff they feel necessary to perform HMIS data entry, data quality or the reporting process.

At this site visit, HMIS staff will document the goals of the prospective HMIS Member Agency in regards to HMIS (what do they want to achieve by using the system), go over the required data elements, review the Policy and Procedures, define entry requirements, and set expectations. The site visit also allows HMIS staff to properly assess the prospective HMIS Member Agency providers workflow and user needs, specific implementation issues, and any constraints or risks that will need to be mitigated by the prospective HMIS Member Agency prior to going live. A site demo using a training version of the HMIS system may also be used (at HMIS staff discretion) during the visit to visually explain HMIS and its capabilities.

Minimal Technical Requirements

Policy 3.7: All HMIS End User workstations must meet minimum technical requirements in order for HMIS to be functional and to meet the required security specifications.

Procedure: The following details are the minimal set of technical requirements for hardware and Internet connectivity to the HMIS system. HMIS works with all operating systems.

Hardware:

- Memory: 4 Gig recommended, (2 Gig minimum), If XP – 2 Gig recommended, (1 Gig minimum)
- Monitor: Screen Display - 1024 by 768 (XGA)
- Processor: A Dual-Core processor is recommended.

Internet Connectivity:

- Broadband Internet Connectivity recommended (High Speed Internet).

Authorized Browsers:

- Firefox 3.5 or greater

- Internet Explorer 8.0 or greater
- Safari 4.0 or greater
- Google Chrome 5.0 or greater

Workstation Maintenance:

- Workstations should have their caches refreshed on a regular basis to allow for proper speed and functionality.
- Workstations should continue to be updated to the most current version of Java, as suggested by their software.
- Workstations may need their virtual memory increased.

HMIS Data Use

Policy 3.8: HMIS Member Agency providers will not violate the terms of use of data within the HMIS system.

Procedure: HMIS Member Agency providers will not breach system confidentiality by misusing HMIS data. HMIS data is not to be used for any purpose outside the use of case management, project evaluation, education, statistical and research purposes.

Policy 3.8.1: HMIS Member Agency providers shall not use any data within HMIS to solicit clients, organizations, or vendors for any reason.

Procedure: At no time shall confidentiality of clients, organizations and vendors be violated by disclosing client information to non-members. Data in HMIS will not be used to solicit for volunteers, employees, or clients of any type. This information must not be sold, donated, given, or removed from HMIS for any purpose that would violate client, organization, or vendor confidentiality or put participants at harm or risk. Those found in violation of this rule will have their access to HMIS immediately terminated and the violation disclosed to all local government and funding entities.

Policy 3.8.2: HMIS Member Agency providers shall not sell any HMIS client, organization, or vendor data for any reason.

Procedure: At no time shall confidentiality of clients, organizations, and vendors be violated by selling any information. HMIS Member Agency providers shall not profit from disclosure of client, organization, or vendor information. Disclosure of information puts everyone at legal risk. Violation or breaches in HIPAA and 42 CFR regulations can result in fines and jail time. Those found in violation of this rule will have their access to HMIS immediately terminated and the violation disclosed to all local government and funding entities.

HMIS Corrective Action

Policy 3.9: If an HMIS Member Agency or any of its End Users have violated any HMIS policy, the HMIS Staff will implement an action plan upon discovery of the violation.

Procedure: Violations in HMIS policy may occur. HMIS Member Agencies will work to ensure violations in policy are prohibited. If a violation is discovered, it is the role of the HMIS staff to swiftly respond in order to prevent further violations from occurring or the current violation from harming clients or other HMIS Member Agencies. The HMIS staff will determine a course of action depending on the type and the severity of the policy violation.

Critical Risk (For example: Security Breach, Imminent risk to clients, Unresolved Data Quality Errors)

- HMIS System Administrator will suspend all HMIS Member Agency Active End User Licenses. Affected End Users will be suspended until retraining.
- HMIS Project Coordinator immediately reports the violation to the HMIS Lead Agency.
- HMIS Project Coordinator will contact the HMIS Member Agency in question to discuss the violation and course of action.
- HMIS Member Agency will be suspended until violation is resolved and will be placed on probation for at least 90 days.
- HMIS Lead Agency will contact the HMIS Member Agency Contract Manager to discuss violation and action plan.

Medium Risk (For example: Grievance has been filed against HMIS Member Agency or general complaints that threaten or endanger clients.)

- HMIS Project Coordinator immediately contacts and reports to the HMIS Lead Agency to discuss the course of action and plan.
- HMIS Project Coordinator will contact the HMIS Member Agency in question to discuss the violation and course of action.
- The HMIS Lead Agency will contact the HMIS Member Agency Contract Manager to discuss violation and action plan.
- HMIS Member Agency will be placed on Probation for at least 90 days and possible suspension until violation resolved.
- If appropriate, HMIS System Administrator will suspend all HMIS Member Agency's Active End User Licenses.

Low Risk (For example: Unresponsive HMIS Member Agency to HMIS Requests, Ceased Data Entry, Incorrect Bed List, End User Inactivity, and Timeliness Issues.)

- HMIS Project Coordinator immediately contacts and reports to the HMIS Lead Agency to discuss the course of action and plan.
- HMIS Project Coordinator will contact the HMIS Member Agency in question to discuss the violation and course of action.
- If appropriate, the HMIS Lead Agency will contact the HMIS Member Agency Contract Manager to discuss violation and action plan.
- If appropriate, HMIS Member Agency will be placed on probation for at least 90 days or until violation resolved.
- If appropriate, HMIS System Administrator will suspend all or some of the HMIS Member Agency End User Licenses in question.

Potential Courses of Action

Probation

The HMIS Project Coordinator will notify the Agency's Executive Director and HMIS Agency Administrator in writing to set up a one-on-one meeting to discuss the violation in question. During the meeting, an action plan will be developed and documented with relevant time frames outlined set to correct actions. If a training issue is identified, the HMIS Project Coordinator will coordinate further follow up with the End Users in question. The Member Agency will be on placed on probation, for a minimum of 90 days, where monitoring and auditing may be required and performed regularly during this period. Notification of probation will be communicated to all local contract managers.

Suspension

If a violation is of critical risk or the corrective measure(s) are not achieved in the probationary period, or more HMIS violations occur during the probationary period, the HMIS System Administrator will suspend access to HMIS until the issues are resolved. The HMIS Member Agency will receive a written notice to the Member Agency's Executive Director of the suspension, reasons, and effective date. During suspension, a mandatory meeting will be held between the Member Agency Executive Director, the CoC Leadership, and the HMIS Staff, if appropriate, to discuss suspension and requirements for resolution. All meeting deliverables will be documented in writing and must be achieved within the set probationary period.

Termination

If the Member Agency violates any policies deemed of critical risk and fails to achieve resolution within the probation period, the HMIS Staff will permanently terminate the Member Agency from HMIS. The HMIS Member Agency will receive a written notice to the Member Agency Executive

Director outlining the termination, reasons, and effective date. Notification of the termination will be sent to all local contract managers. In the case of incurred data quality costs and/or transfer costs, the Member Agency will assume responsibility for payment.

Section 4: User Administration

HMIS End User Prerequisites

Policy 4.1: All HMIS Users are required to have minimum set of basic computer competency and skills to adequately perform their data entry roles in HMIS.

Procedure: Each HMIS Member Agency Administrator should meet the skill requirements set forth in the Agency Administrator Minimum Qualifications White Paper. All other HMIS Users should be prepared with basic computer competency/skills to adequately be able to use and navigate HMIS. Users will be evaluated for competency at the beginning of training. Users who do not have a minimum competency will be asked to leave training and seek a basic competency class. Basic computer competency classes can be found at a local library, community center, college, or business learning center. Once the user has completed the basic competency class, they can register and attend HMIS training. Upon return, they will be required to produce proof of attendance at the basic computing class.

Policy 4.2: All HMIS Users should have had a background check prior to being assigned access to HMIS by a HMIS Member Agency.

Procedure: HMIS Member Agency providers are encouraged to have background checks on all staff and volunteers prior to assigning them access to HMIS. HMIS Member Agency shall review the received criminal history report before the end user signs-up for HMIS training. Background checks that come back with a criminal history should be carefully considered prior to giving them access to client information. **See policy 4.3.**

HMIS End User Agreement

Policy 4.3: No prospective HMIS User will be given a license for HMIS if she or he has entered a plea of nolo contendere (no contest) or been found guilty of any fraud (including identity theft) or stalking related felony crimes punishable by imprisonment of one year or more in any state.

Procedure: A HMIS Member Agency should not risk the privacy and confidentiality of client information by allowing any individual convicted of a fraud or stalking related crime (fraud, identity theft, stalking) in any state. In the broadest sense, a fraud is an intentional deception made for personal gain or to damage another individual. An HMIS User needs to be mindful of potential identity theft and improper usage and disclosure of client information. This policy will be taken under consideration and possibly waived if the prospective user has passed a State of Tennessee Level II Background Check.

An HMIS User will be denied HMIS access if they meet any of the following, whether a judgment of guilt was withheld or not:

- has entered a **plea of nolo contendere** (no contest) to a fraud related felony crime (fraud, identity theft, stalking) punishable by imprisonment of one year or more.
- has entered a **plea of guilty** to a fraud-related felony crime (fraud, identity theft, stalking) punishable by imprisonment of one year or more for crimes concerning.
- has **been convicted or found guilty** of a fraud related felony crime (fraud, identity theft, stalking) punishable by imprisonment of one year or more for crimes.

Policy 4.4: Any prospective HMIS User who was a previous client of the same project he or she now intends to work or volunteer must not have resided at the facility or been a project participant in the last 6 months prior to gaining access to HMIS.

Procedure: The HMIS User for most residential/homeless service projects must not have been a previous client of the same project he/she now intends in which work or volunteer for last 6 months prior to gaining access to HMIS. An HMIS User should never have access to detailed information on project/service participants that may have received services at the same time as the end user. Any HMIS Member Agency who violates this rule is putting client information at risk of a privacy and confidentiality breach. Upon discovery of the practice, HMIS Lead staff will immediately inactivate the HMIS User in question and notify the agency administrator and end user of the inactivation in writing.

Policy 4.5: All HMIS Users must be provided with a software license by and provided training through the HMIS staff prior to entering or accessing client data in HMIS.

Procedure: Due to the amount of personally identifying information and the confidential nature of the HMIS, every HMIS User must be assigned a software license to access the system and their initial training must come from the HMIS Lead staff. In order to receive a license, a potential HMIS User must not violate HMIS policies 4.0 through 4.4. Furthermore, a condition of being granted a license is that all users must sign and adhere to an HMIS User Agreement. This document outlines the role and responsibility of having and maintaining their access in HMIS. An HMIS User who violates the HMIS User Agreement will be immediately inactivated from HMIS and required to attend re-training to re-gain access.

License Administration

Policy 4.6: Notification of issuance and revocation of access within the HMIS is the responsibility of Agency Administrator.

Procedure: Agency Administrators are responsible for notifying the HMIS Lead staff of a new user, change in user access, or deletion of user access within 24 business hours of their organization's needed change. Agency Administrators should work with the HMIS Lead staff to ensure proper license access is given to qualified HMIS Users. However, only HMIS Lead staff can complete issuance, maintenance, and revocation of software license.

Assignment of End User security settings

The HMIS Lead staff will assign the security level of every end user based on the agreed upon security settings established by the Member Agency at the Initial HMIS site visit. The Agency Administrator or Executive Director will assign access to individuals based on their role in the organization and needed access to HMIS. Assignments are best organized by the lowest level of security the staff or volunteer member would need to perform their normal work duties as defined by their official job/position description. If the HMIS User is to remain on the system, but has had a change in responsibilities, an Agency Administrator or Executive Director may request a change in any end users security setting.

Additional licenses/changes.

All requests for new licenses must be submitted to the HMIS Member Agency Administrator or the HMIS Lead Agency. Request forms must be received and approved no later than 72 hours before the scheduled training date. All new licenses are issued only after a MOU and HIPAA Agreement have been signed by the HMIS Member Agency and the HMIS End User Agreement has been signed by the appropriate HMIS User. Licenses are allocated on a first come-first served basis based upon agency size, use, and adherence to all Policies and Procedures set forth in this document. If there are no more licenses available, the user will have to wait until a license is available or the HMIS Member Agency may purchase a license for the HMIS User.

Inactivity

An HMIS User must successfully complete all assigned training homework within 5 business days after the initial training date and allow no more than 60 days between login sessions on the live site to keep their license active. Any HMIS User who is in violation of these rules will have their access inactivated by HMIS Lead staff immediately and the user will be required to attend re-training in order to regain access. They may be charged a license fee. If a license is no longer needed by the Member Agency, it will be distributed to the pool of available licenses open to all Member Agency providers. An inactivity report can be generated and shared with the Agency Administrator upon request.

HMIS Lead Staff removing a user license for cause

HMIS Lead reserves the right to inactivate or delete the license for any end user for cause. In all cases where a licensee is removed for cause, the assigned HMIS Member Agency Administrator and Executive Director will be notified immediately via email with the stated cause of license removal. Reasons that a licensee would lose their license or otherwise have their license temporarily inactivated or revoked would include, but not be limited to:

- Multiple failed logon attempts in the same day.
- A consistent lack of good data quality.
- Three consecutive no call, no shows to scheduled training.
- Failure to log on to system at least once in a consecutive 60 day period.
- Sharing system credentials (login and password) with any other party.

- Allowing non-authorized users to view any data from, have access to, see the screens of, or be provided any print outs of client data from HMIS.
- Other violations of these HMIS Policies.
- Other serious infractions that result in a compromise of the HMIS Member Agency and/or any client level data in the system.

Agency removing a user license

An HMIS User license can only be deactivated by the HMIS Lead staff. Requests for removal of a license by a HMIS Member Agency can only come from the Agency Administrator or Executive Director and the request must be submitted in writing through the HMIS User License Request Form. All license requests should be communicated to HMIS within 24 business hours after the end user has left the employment of the HMIS Member Agency, the HMIS User has changed positions and is no longer in need of HMIS access, or has knowingly breached or is suspected of a system breach where client data has been compromised. Terminations should be submitted using the HMIS License Request Form.

Law Enforcement

Policy 4.8: No active member of law enforcement or detention and corrections staff will be an authorized HMIS User.

Procedure: To protect current clients who may be accessing health and human service projects from harassment or harm, active members of law enforcement will not be granted access to HMIS. Limited exceptions may be negotiated and an agreement executed with HMIS, the local CoC, when there is a project with direct involvement in an active homeless jail diversion and/or prison release project. Any agreement with exceptions must include a statement that: HMIS use is (1) limited to the purpose for which it was intended; and (2) is only for work with project involved clients.

Former members of law enforcement who may volunteer or are employed at a homeless service provider post-law enforcement career may have access to HMIS if it is imperative to their new responsibilities. HMIS will consider and respond to requests by law enforcement with next of kin searches, searches for clients and in the interest of public safety a person(s) who law enforcement has probable cause or an active warrant for his/her arrest related, to a violent crime and other felony crimes. HMIS will provide law enforcement information related to evidence and information gathering concerning a criminal matter via Court Order, such as a search warrant or subpoena.

Section 5: Clients' Rights

Client Consent

Policy 5.1: An HMIS Member Agency must obtain consent from all clients for whom they are entering or accessing client data into HMIS.

Procedure: No client shall be entered into HMIS without their written consent. The HMIS Member Agency agrees to get written permission on one or both of the following forms signed by the client: Notice to Clients of Uses and Disclosures and/or a Release of Information. All consent forms are not system-wide, but specific to the project/service they are receiving.

Notice to Clients of Uses and Disclosures

The HMIS Client Notice to Clients of Uses and Disclosures form provided is required to be used to record a client's authorization for their data to be entered into HMIS. The original signed Notice to Clients form should be kept by the HMIS Member Agency and protected from theft or loss. This form explains to clients their rights and authorizes the data to be entered into HMIS. HMIS End Users should strive to communicate the contents on the form in a language the client understands. The Notice to Clients form must be completed by each member of the household receiving services who is over the age of 18. The Head of Household may sign for all members of the household under the age of 18 on the same form. Member Agencies are responsible for establishing an expiration date for the consent, as well as securing updated forms after expiration and updating them in HMIS. It is important to understand that agencies cannot deny services to individuals solely on the basis of the individual deciding not to share information in HMIS.

Release of Information (ROI)

The HMIS Release of Information (ROI) form is used to control how client data is shared in HMIS. It should be kept by HMIS Member Agency and protected from loss of theft. Member Agencies are required to use the HMIS Release of Information form provided. Release of information is specific to sharing data among providers in the Continuum of Care, as well as HMIS Member Agencies. Clients have the right to have their records open, partially open or closed. HMIS Users should strive to communicate a Release of Information in a language the client understands. The form must be completed by each member of the household receiving services who is over the age of 18; and those who did not sign the Notice to Clients of Uses and Disclosures. The head of the household may sign for any children or members of the household under the age of 18 on the same form. If the client is still receiving services when the ROI expires and the client chooses not to sign the Informed Consent, but still wants to control how their data is shared, they will need to sign another HMIS Release of Information form and the data will need to be updated in HMIS.

Agencies must make reasonable accommodations for persons with disabilities throughout the data collection process. This may include, but is not limited to, providing qualified sign language

interpreters, readers or materials in accessible formats such as Braille, audio, or large type, as needed by the individual with a disability.

Agencies that are recipients of federal assistance shall provide required information in languages other than English that are common in the community, if speakers of these languages are found in significant numbers and come into frequent contact with the project.

Client Access to Information

Policy 5.2: All clients entered into HMIS have a right to view information within their electronic HMIS file.

Procedure: If an HMIS Member Agency has a written policy for providing copies of their paperwork or data collection to clients, the HMIS Member Agency may follow its procedures to allow for providing copies of the HMIS data they collected. Clients can request a copy of their information in writing to the HMIS staff through email or regular mail. Once received, the HMIS staff will fulfill the client's request in an expedited manner.

Filing a Grievance

Policy 5.3: Clients have the right to file a grievance with the HMIS staff about any HMIS Member Agency related to violations of access in HMIS, violations of HMIS Policies and Procedures, or violations of any law.

Procedure: HMIS staff will entertain any client who wishes to file grievance against any HMIS Member Agency. HMIS staff will request that a client fill out a HMIS Client Grievance Form, which can be obtained by contacting the HMIS staff by phone, email or regular mail. Once completed and submitted by the client, HMIS Staff will investigate the complaint and provide its findings to the client who lodged the grievance. HMIS will notify the parties involved about the alleged incident reported. If the client is not satisfied with the findings of the grievance, the client must submit a grievance request in writing to the U.S. Dept. of Housing and Urban Development.

Policy 5.4: Other HMIS Member Agencies have a right to file a grievance with the HMIS staff about any HMIS Member Agency related to violations of access in HMIS, violations of HMIS Policies and Procedures, or violations of any law.

Procedure: HMIS staff will entertain any HMIS Member Agency who wishes to file grievance against any other HMIS Member Agency. In cases where a client leaves one HMIS Member Agency to receive services from another HMIS Member Agency and the client reports a suspected violation, the new HMIS Member Agency does have a right to file a grievance or duty to warn the HMIS staff on behalf of the client as long as the client grants their permission to file a grievance on their behalf. HMIS staff will request a HMIS Client Grievance Form be completed by either the client or the HMIS Member Agency. The form can be obtained by contacting the HMIS staff by phone, email or regular mail. Once completed and submitted by the client, HMIS Staff will investigate the complaint and provide its findings to the client who lodged the grievance. HMIS

staff will notify the parties involved and the appropriate community planners about the alleged incident reported. If the client is not satisfied with the findings of the grievance, the client must submit a grievance request in writing to the U.S. Department of Housing and Urban Development.

Revoking Authorization for HMIS Data Collection

Policy 5.5: All clients who initially agree to participate in HMIS have the right to rescind their permission for data sharing in HMIS.

Procedure: Clients who choose to revoke their information sharing authorization must complete a new Release of Information. The new Release of Information should be sent by the Agency Administrator who will notify the HMIS Staff that the client record is to be “closed” in the system. The HMIS staff will be responsible for closing the client record from view.

Once closed, the HMIS Member Agency will no longer be able to share future client data entered into HMIS. However, data entered prior to the record being closed can still be viewed and shared with other Member Agency providers. The new Release of Information should be kept on file by the Member Agency. After a Release of Information is signed and a client is accepted into a HMIS participating financial assistance project, the client must sign a client consent form and HMIS staff must be notified to re-open the client record for sharing. The notification to re-open the file must be submitted in writing, along with a scanned copy of the client’s newly signed consent.

Section 6: Privacy, Safety & Security

National Privacy Requirements

Policy 6.1: HMIS complies with all federal, state, local laws, standards, and regulations.

Procedure: It is imperative that partner agencies have Policies and Procedures in place that ensure compliance with applicable laws and regulations that govern their projects.

HIPAA Covered Entities

Any Agency that is considered a “covered entity” under the Health Insurance Portability and Accountability act of 1996, 45 C.F.R., Parts 160 & 164, and corresponding regulations established by the U.S. Department of Health and Human services is required to operate in accordance with HIPAA regulations. More information about 45 C.F.R. may be found at:

<http://www.hhs.gov/ocr/privacy/>

42 CFR Part 2 Entities

Any Agency that is considered a “covered entity” under 42 C.F.R. Part 2, and corresponding regulations establishing by the U.S. Department of Health and Human Services is required to operate in accordance with the corresponding regulations. More information about 42 C.F.R. may be found at: http://www.access.gpo.gov/nara/cfr/waisidx_02/42cfr2_02.html

Domestic Violence (DV) Shelters

Any agency that is a victim service provider is barred from disclosing identifying information to HMIS as of 2007. More information about DV Shelters and HMIS may be found at:

<http://epic.org/privacy/dv/hmis.html>

Other Entities

Any Agency that is NOT considered a “covered entity” under any of the above mentioned projects is required to operate in accordance with HMIS/HMIS privacy and security rules, as well as any applicable federal, state, local laws and regulations. More information about HMIS Privacy and Security Rules may be found at:

https://www.hudexchange.info/resources/documents/HEARTH_HMISRequirementsProposedRule.pdf

Privacy Notice

Policy 6.2: HMIS Member Agency providers must post a HMIS Privacy Notice prominently on their websites and in areas of plain view of the public such as waiting rooms, intake areas, lobbies, or screening or assessment areas. HMIS Member Agency providers are required to provide a copy of the HMIS Privacy Notice to all clients upon request by the client.

Procedure: By law, HMIS Member Agency providers are required to post a Privacy Notice that discloses collection and use of Client Information. HMIS has developed a document for posting

for providers without an adequate notice. The HMIS Privacy Policy and Notice are document in the Appendix of this document.

System Security and Privacy Statement

Policy 6.3: The HMIS Lead Agency has implemented extensive technical and procedural measures to protect the confidentiality of personal information while allowing for reasonable, responsible, and limited uses and disclosures of data as recommended in the HMIS Data and Technical Standards.

Procedure: The security and confidentiality of homeless and at-risk client information within HMIS is a major issue. For certain providers and sub-populations, such as Domestic Violence Shelters, Substance Abuse Facilities, and HIPAA Covered Entities, security and confidentiality of client information becomes even a much larger concern for all involved. The HMIS Data and Technical Standards, published June 30, 2004 and updated through 2014 by the U.S. Department of Housing and Urban Development (HUD), include extensive HMIS Privacy and Security Standards to be followed by Continuum of Services, Homeless Assistance Providers, and HMIS Software companies. These standards were developed after careful review of the Health Insurance Portability and Accountability Act (HIPAA) standards for securing and protecting patient information. The HMIS has and will continue to be in compliance with these Privacy and Security Standards even while not being considered a HIPAA covered entity as an HMIS Lead Agency.

Policy 6.4: HMIS secures the location of the server in a controlled hosting environment providing security from data loss and theft.

Procedure: HMIS contracts with a HUD approved software vendor to provide HMIS to the Continuum of Services. As a web based HMIS solution, the HMIS software and databases are hosted on secure servers in a highly secure computer room accessible only by very few employees who are responsible for maintaining and supporting the system. The vendor computers are also protected by firewalls to prevent unauthorized external access.

Policy 6.5: HMIS ensures that only appropriate staff and volunteers at HMIS Member Agency providers gain and retain system access through a user authentication process.

Procedure: As an Internet based software system, each HMIS User accesses the system via their internet web browser. To access HMIS, each user must know the web address (URL) for HMIS, which is not available or published outside the community.

Once on the website, each user must use a valid user sign on and dynamic password. All user names and initial temporary passwords are issued by HMIS staff only. Passwords are considered expired every 45 days and users are prompted for new dynamic passwords. Additionally, after three failed logon attempts, user ID's and passwords automatically become inactive and users

must contact an Agency Administrator or HMIS staff for reactivation. Passwords are always encrypted and can never be seen in clear text.

Policy 6.6: HMIS secures data as it is traveling over the Internet and stored on the centralized server by providing encryption for all data.

Procedure: As a cloud or web based software system, it is imperative that all data travel through the Internet encrypted or unreadable to an outside user. All HMIS transactions are fully encrypted using Secure Socket Layer (SSL) with 128-bit encryption. This is the highest commercially available encryption level and is the same as used by financial institutions. Users can be assured that the data they are interacting with is secure by noticing the URL, or Web Address while using HMIS begins with the letters HTTPS (Hypertext Transfer Protocol Secure).

Policy 6.7: HMIS staff, in conjunction with the HMIS Member Agency Administrator, ensures that all HMIS Users have access to the components of the system appropriate for their level of data usage.

Procedure: The HMIS software has a built-in security system that ensures each user only has the minimum access needed to perform their normal duties. Each HMIS User is assigned a security level in their user profile that grants them access to only the areas they need to accurately do their work. A change to the level of system security for an end user may only be requested by an Agency Administrator or Executive Director for which the end user works.

Policy 6.8: HMIS staff use audit trail tools to ensure system maintenance, investigate privacy, security breaches or filed client grievances.

Procedure: The HMIS software has built-in audit trail applications that allow administrators to audit use and access of data. Audit reporting is an integral part of maintaining system security protocols and is performed on a scheduled basis by HMIS staff.

Policy 6.9: The HMIS is a shared information system with default visibility and security exceptions preset by HMIS staff based on the workflow of the Member Agency.

Procedure: Pursuant to 42 and 45 CFR notwithstanding, HMIS is an open or shared HMIS system. The default visibility settings for clients will be set to OPEN for all HMIS clients that are not registered or receiving services from any 42 or 45 CFR facility or project. If client is enrolled in a 42 or 45 CFR covered entity project, project visibility settings will be set in accordance to applicable laws.

The HMIS system utilizes a set of Visibility Settings that allow sharing of only agreed upon data elements among the participating HMIS Member Agencies. The HMIS system utilizes a set of Deny Exceptions that disallow sharing of certain information by provider projects based upon federal, state, or local laws and guidelines, and by agreement with each HMIS Member Agency provider. System Visibility settings may only be changed by the HMIS staff. Requests to change visibility settings must be made via written request to HMIS staff. The HMIS System is

constructed to offer a dynamic range of levels of security based on the needs of the agency and HMIS User. As a default, HMIS Users will only have enough security access to perform their normal job duties. Requests to change a user status must come from an HMIS Member Agency Administrator or Executive Director.

A client has the right to refuse to have his or her data entered into the HMIS database. The client's individual choice regarding participation will not affect his or her rights to services.

Data Ownership

Policy 6.10: All data is governed by the owner(s) of the data with regard to data use and disclosure.

Procedure: The client ultimately retains ownership of any identifiable client-level information that is stored within HMIS. If the client consents to share data, the client, or agency on behalf of the client, has the right to later revoke permission to share her or his data without affecting rights to service provision.

Section 7: User Training

HMIS Training Process

Policy 7.1:

All HMIS Users are required to have a basic computer competency prior to attending any HMIS training.

Procedure: Prior to being sent to HMIS training, all HMIS Users should have basic computer competency. HMIS Users should be able to turn on/off a computer, use a mouse and keyboard, launch a browser, enter a URL, and navigate the World Wide Web. HMIS Users who cannot complete these tasks should be sent to a basic computer competency class prior to being scheduled for HMIS training. HMIS staff will verify the competency of all Users prior to training.

Policy 7.2: HMIS Lead Agency has established beginning, advanced, and ongoing training requirements for system users and agency administration.

Procedure:

Beginning Training

1. System users *must* attend Beginning Training before accessing the system. Beginning Training is designed to give users an introduction to the system.
2. A staff person may attend a specific training, depending on their role within the agency. Training modules are developed on skill level and type of access to the system.
3. Under no circumstances should anyone in the agency who has not received official training by HMIS Administration have access to or use the HMIS.

Privacy Training

Privacy Training, which has now been integrated into the Beginning Training curriculum, is mandatory for all system users. This training is designed to ensure that the user safeguards the privacy/confidentiality of the client when accessing the system. The user is instructed on obtaining Client Consent/ Release of Information and the appropriate use and disclosure of client data. The user also receives instruction on maintaining the privacy of his/her username and password.

Reporting Training

Training for canned and customized reports is available to advanced users. This training must be requested by the HMIS Member Agency.

Onsite Training

HMIS staff is available to deliver onsite training in the event that an agency has a large number of staff to train or wants a specific topic covered.

Section 8: HMIS Technical Support

Policy 8.1: The Homeless Management Information System staff will provide a system that will allow HMIS Users to request technical assistance, general HMIS related inquires, training and workflow questions, and data quality assistance.

Procedure: All requests for technical assistance must be submitted through the HMIS help desk tracking system or email. All tickets or emails will be answered during normal HMIS business hours, Monday through Friday, 8:30 am to 5:00 pm.

Policy 8.2: The HMIS staff will respond to all inquiries from Member Agencies and clients in a timely manner.

Procedure: Response times for technical assistance varies based on the item that is submitted and the priority associated. HMIS Staff reserve the right to adjust priority levels based on the type of the request.

Normal Business Hours

Requests for routine system technical support will be honored on a first come-first served basis categorized in the following manner:

Issue Type	Type Definition	Tool to Report	HMIS Staff Response
Rapid Response	Users are unable to use system. For example: the system is down or the site is unreachable.	Submit a service request or contact staff by phone.	Immediate. No less than 12 hours.
Priority Response	Users can use the system, but one or more functions important to day-to-day operational use is severely affected. For example: password issues, permission issues, security issues, not accepting data, or screens have changed.	Submit a service request via email or helpdesk.	Less than 24 hours.
Regular Response	A problem is noted, but users are able to use all functions in the systems without major difficulty. For example: reporting issues, general questions, work flow issues, data entry problems, change to a report, or change to screens.	Submit a service request via email or helpdesk.	Less than 48 hours.
Feature Enhancement	Users are able to use all functions in the system as normal, but are requesting an enhancement to the system that is currently not available.	Submit a service request via email or helpdesk.	Less than 48 hours.

After Hours

After hours and weekend requests will be treated as if the request was received at opening of the next business day. HMIS staff normal working hours for Technical Assistance are Monday through Friday, 8:30 am through 5:00 pm. Each HMIS can fill in hours. For after-hour requests, please contact your Agency Administrator.

Policy 8.4: HMIS staff will submit to the vendor all feature enhancement requests submitted through the proper channels from Agency Administrator(s) or HMIS Users.

Procedure: It is a stated goal of HMIS to be as efficient and user-friendly as possible within the technical restraints of the system. Feature enhancement requests are welcomed and encouraged. Please submit all possible feature enhancements in the following manner:

- Begin by submitting a service request to a technician.
- Code the request type as a feature enhancement.
- Be as specific as possible in the request.
- If appropriate, describe the current workflow first and the suggested feature enhancement right after.
- If enhancement is for new system functionality, please describe a workflow and diagram as much as possible.
- If appropriate, please denote how much time savings would be achieved if the feature enhancement were to be enacted.
- If appropriate, please denote all of the possible benefits for your agency or End Users and other Member Agency providers if feature enhancement were to be enacted.

Policy 8.5: The HMIS System staff will hold mandatory periodic in-person meetings or conference calls to discuss system changes and provide technical support.

Procedure: Agendas will be driven by submitted requests for agenda or discussion. All information, including agenda and instructions, will be sent to agency administrators via e-mail at least 48 hours before the meeting. All attendance records are open to review by local government entities and other community planners.

Section 9: Data Collection Process

Clients Served vs. Clients Benefiting from Service

Policy 9.1: All client data entered into HMIS by the Member Agency should be that of clients receiving services and/or its family in attendance.

Procedure: Clients entered into HMIS should consist of the clients in attendance at the day of enrollment into the project or services, and can consist of minors under the age of 18 if the legal guardian consents to their entry into HMIS. HMIS is not meant for adult clients who are not in attendance or may benefit from services at a later date. HMIS Member Agency providers should refrain from entering adult clients into HMIS that are not physically seen to be enrolled in the project or provided the service because they cannot give consent in absentia. For those providing financial assistance services per address, it is expected each member of the household receiving the service by the same address must provide consent and be entered as a household unit in HMIS and linked together using a service transaction, otherwise there is a risk of duplication of services. Data on all members of the family should be entered individually, but tied together as a household. The head of household can give consent for all minor children (under 18 years of age) in a family but cannot give consent for any adult members (over the age of 18). All adults must give their consent individually.

Data Entry Requirements

Policy 9.2: The HMIS staff requires each HMIS Member Agency to enter client level data based on a set of predefined data standards.

Procedure: HMIS data standards are based on the most current revision of the HUD Homeless Management Information System (HMIS) Data Standards. Every project entering into HMIS must adhere to the requirements set by HUD and the local Continuum of Care. Every project entering data into HMIS is evaluated based on the following elements: completeness, consistency, accuracy, and timeliness. *Refer to Section 10 on Data Quality for details.*

Procedure for All Projects

Every HMIS Member Agency is required to enter the following Universal Data Elements as outlined in the 2014 HUD Data Standards in order to meet minimum data entry standards. The elements required for every person who is entered in the system are:

Release of Information documented, Full Name (First, Last), Name Data Quality, Social Security Number (full or partial), Social Security Data Quality, Date of Birth, Date of Birth Data Quality, Primary Race, Ethnicity, Gender, Veterans Status, Disabling Condition, Residence Prior to Project Entry, Length of Stay in Previous Place, Project Entry Date, Project Exit Date, Zip Code, Relationship to Head of Household, Client Location, Length of Time on the Street, Continuously

Homeless for One Year, Number of Times the Client Has Been Homeless in the Past Three Years, and homeless status verification documented.

Procedure for McKinney-Vento Funded Projects

HMIS Member Agencies who are funded through any of the programs below must meet the basic requirements set by HMIS and also meet additional Program Specific Data Elements (PSDE). Found at HUDHRE.com and <https://www.hudexchange.info/>

- Emergency Solutions Grant (ESG);
- Supportive Services for Veteran Families (SSVF)
- VA Grant and Per Diem Program (GPD)
- Rapid Re-Housing Program (RRP);
- Projects in Assistance of Transition from Homelessness (PATH);
- Supportive Housing Program (SHP);
- Shelter Plus Care (S+C);
- Section 8 Moderate Rehabilitation for Single Room Occupancy (SRO);
- Housing Opportunities for Persons with AIDS (HOPWA).

Additional program specific data elements to be collected are detailed in the 2014 HUD Data Standards and vary by program type (e.g. PATH, SSVF, RHYMIS, ESG, etc.) and may include: Housing Status, Income Amount, Income Source(s), Income Date(s), Non-Cash Benefits, Non-Cash Benefits Source(s), Non-Cash Benefits Date(s), and Sources, Health Insurance, Health Insurance Source(s), Health Insurance Information Date, Reason for No Health Insurance (if applicable), Disability Type, Domestic Violence Victim/Survivor, Domestic Violence Information Date, Contact Date (Street Outreach Only), Date of Engagement (Street Outreach and Services Only Projects), Services Provided (PATH, HOPWA, & VA Funded), Financial Assistance Provided (HPRP only), Referrals Provided, Residential Move-in Date, Housing Assessment Disposition), and Housing Assessment at Exit.

All providers receiving HUD funding must have at least one service transaction per client (for HPRP must have at least one service transaction under Financial Assistance and at least one under Housing Relocation and Stabilization). The housing status must be recorded at project entry. The PSDE of income and sources must be recorded at project entry and verified at least one time during a year if in the project over a year.

It is recommended that Member Agencies and Agency Administrators review the 2014 HUD Data Standards (<https://www.hudexchange.info/resources/documents/HMIS-Data-Standards-Manual.pdf>) and Data Dictionary ([KnoxHMIS Policies & Procedures, Version 5: July 1, 2017](https://www.hudexchange.info/resources/documents/HMIS-</p></div><div data-bbox=)

Data-Dictionary.pdf) to ensure that their specific projects are collecting all required project specific data elements as designated by funding stream(s).

Managing Bed Inventory (*Housing Providers Only*)

Policy 9.3: All Housing Providers are required to maintain the most current bed inventory in HMIS. HMIS must be notified at least 5 days in advance of a change to any beds at the facility and client inventory in HMIS in real-time must reflect the most current project utilization.

Procedure: All Housing Providers must work with HMIS Staff to build accurate bed lists in HMIS. Each HMIS bed list should be assigned to the appropriate project (Emergency, Transitional, Permanent Supportive, etc.). If there are any changes to the bed lists, the Agency Administrator is required to notify the HMIS System Administrator at least 5 business days prior to the beds becoming available. Clients being assigned to beds or exited from beds in the system should be done in real time as the client is entering the project. In cases where clients are unable to be entered or exited in real time due to technical difficulties, all data must be current within 24 hours. Clients entering as families must be built as families in HMIS prior to bed entry and must be assigned together as part of the ShelterPoint module.

Optional Requirements

Policy 9.4: All Member Agency providers are encouraged to record all Program-Specific Data Elements (PSDE) for all clients entered into HMIS even if not required for funding.

Procedure: Optional PSDE is a valuable area of the client record and part case management. Therefore, though not required, HMIS Users are encouraged to complete these elements for each client, especially if the client is in a housing or financial assistance project. The optional PSDE include: Employment, Adult Education, General Health Status, Pregnancy Status, Veteran's Information, and Children's Education.

Client Self-Sufficiency Outcomes Matrix

Policy 9.5: Case Managers are encouraged to use the HMIS Client Self-Sufficiency Outcomes Matrix as an assessment tool for all clients that are entering and exiting a project.

Procedure: The Client Self-Sufficiency Outcomes Matrix is a newly offered optional assessment tool for each client in the HMIS system. The matrix is built with a series of assessment domains that a case manager may use to evaluate the strengths and weaknesses of a client as they begin and continue their case plans and assistance strategies. The domains to choose from include the following: Income Domain, Employment Domain, Shelter Domain, Food Domain, Childcare Domain, Children's Education Domain, Adult Education Domain, Legal Domain, Healthcare Domain, Life Skills Domain, Mental Health Domain, Substance Abuse Domain, Family Relations Domain, Mobility Domain, Community Involvement Domain, Safety Domain, and Parenting Skills Domain. Case Managers utilizing this tool usually pick a series to focus on and then complete at

entry, at several points during interim and finally at exit. Client Self-Sufficiency Outcomes Matrix training is part of Level 2 = Case Management training.

HMIS Client Photo ID Cards

Policy 9.6: Member Agency providers are encouraged to create and disseminate HMIS Client Photo ID Card for all clients being entered into HMIS.

Procedure: Some Continuums of Care have established the HMIS Client Photo ID Cards as the identification for all homeless clients in the system. Homeless and at-risk of homeless clients will be issued a HMIS Client Photo ID Card at their first point of entry into the Continuum of Care. The cards may be issued at major continuum points of access such as day centers and one-stop centers or by other Member Agency providers when a service is rendered.

Policy 9.6.1: HMIS Member Agency providers are encouraged to accept the HMIS Client Photo ID Cards for all clients for which they are providing services as proof of ID.

Procedure: In order for the Continuum of Services and clients to see the benefit of ID cards, HMIS Member Agency providers should be willing to generate, accept and ask for HMIS Client Photo ID Cards from clients. This will require some education to the clients about the use of the ID cards and how it will help them access services better. HMIS Client Photo ID Cards are covered in Level 3 training on SkanPoint.

Policy 9.6.2: HMIS Member Agency providers are encouraged to use the HMIS Client Photo ID Cards for all clients for which they are providing services as proof of ID to rapidly check them into services and projects.

Procedure: Using the barcode on the HMIS Client Photo ID Cards, scan technology can help HMIS Member Agency providers do business better. For low volume providers, scan technology can be used to access client records more quickly. For high volume providers, scan technology can be used to check people into like services rapidly.

Section 10: Data Quality

Data quality is **vital** important to the success of the Homeless Management Information System. HMIS Member Agency providers and HMIS staff will work diligently on adhering to the most current revision of the HUD HMIS Data Standards in order to ensure that reports both at the provider level and the system level are complete, consistent, accurate, and timely. Adherence to set data quality standards will help bring additional funded dollars into our community as well as ensure our data reflects our community's level of service when reported locally, statewide, or nationally. Data quality will be evaluated on accuracy, completeness, consistency, and timeliness. This data will be used by the Continuum of Care to monitor progress towards meeting its indicators.

Policy 10.1: The Homeless Management Information System staff will evaluate the quality of all HMIS Member Agency data on the accuracy of the data entered monthly.

Procedure: Accuracy is the degree to which data correctly reflects the client situation or episode as self-reported by the client.

Policy 10.1.1: All client data entered into HMIS should reflect what the client self-reported or an accurate assessment of known information by a case manager, where indicated by the 2014 HMIS Data Standards or most current revision of the HUD HMIS Data Standards.

Procedure: Data captured for entry into HMIS should be what was client self-reported or data known by case managers. HUD Procedures allow case managers to make changes to client data not reported by the client. Client self-reported means any information reported to staff by the client.

Policy 10.1.2: All client data entered into HMIS should be congruent with program details.

Procedure: Client records entered into HMIS should reflect the client population served, match capacity of enrollment, project type, and entry/exit should fall within service parameters. This information is based on consistency of accurate data entered on clients receiving services. For example, if you:

- are a project for men, you should not enter data on women.
- are a state program and state you have 20 beds, there should not be any more than 20 people in shelter unless you are using the overflow beds.
- are a fully HUD funded project, you should only have entry/exit type of HUD.

Policy 10.1.3: While HUD has defined HMIS as the 'record of record', if agencies use paper-based files, they must match information entered into HMIS.

Procedure: All client data entered into HMIS should match the information captured and filed in the HMIS Member Agencies client record/case file. Observed discrepancies could be subject to audit by HUD, HMIS staff, a local government entity or other community planner.

Policy 10.2: The HMIS staff will evaluate the quality of all HMIS Member Agency data on the completeness of the data entered using detailed Data Quality Reports (DQRs), agency reports, and other tools utilized by local HMIS Administrators.

Procedure: Completeness is the level at which a field has been answered in whole or in its entirety. Measuring completeness can ensure that client profiles are answered in whole and that an entire picture of the client's' situation emerges.

Policy 10.2.1: For all clients served and entered into HMIS, a HMIS Member Agency must maintain HUD mandated data quality standards.

Procedure: It is expected that HMIS Member Agencies work to maintain no more than 5% missing data for each HUD Universal Data Element, and PSDE if applicable. The HMIS monthly Data Quality Reports, agency reports, and other tools utilized by local HMIS Administrators will be used to address data quality issues with the HMIS Member Agencies. HMIS staff will work collaboratively with Member Agencies to address and improve overall data quality.

Policy 10.2.2: For all clients served and entered into HMIS by a HMIS Member Agency, no more than 5% of all client level data should be "blank/not reported/null".

Procedure: It is expected that HMIS Member Agencies will work with clients to capture all necessary data. HMIS Member Agencies will be expected to have no more than 5% of all client data "blank/not reported/null" value rate for all clients entered into HMIS (or 95% or above completeness). "Blank/not reported/null" values include fields that are left blank or answered with a client doesn't know, client refused, or data not collected. While these options may accurately reflect what the client has self-reported, they are considered of a low quality value.

Policy 10.2.3: For all clients served and entered into HMIS by a HMIS Member Agency, all system data quality fields must be completed.

Procedure: In HMIS, there are several data quality fields that are essential to understanding patterns of data entry and client self-reporting. These fields are part of the Universal Data Element (UDE) requirements measured for each HMIS Member Agency.

These fields measure the quality of their associated fields. For example, if the Date of Birth field has been left blank, the Date of Birth Data Quality field is used to explain why the field is blank. There are four quality fields in the system.

- Name Data Quality
- Social Security Data Quality

- Zip Code of Last Permanent Address Data Quality
- Date of Birth Data Quality

These fields allow for reporting only partial answers or full answers in order to receive completeness credit. These fields in conjunction with the associated data element field will be used to assess data quality issues.

Policy 10.3: The Homeless Management Information System staff will evaluate the quality of all HMIS Member Agency data on the consistency of the data entered.

Policy 10.3.1: All HMIS Member Agency client data should work consistently to reduce duplication in HMIS by following workflow practices outlined in training.

Procedure: HMIS Member Agencies are trained to search for existing clients in the system before adding a new client into the system by either Name, Social Security Number, and Client Alias. HMIS staff review duplicate data entries in the system and have to merge client records. When duplicate client records created by HMIS Member Agency providers are discovered, the HMIS staff will contact the designated Agency Administrator to notify and address the user creating the duplication. HMIS users can also contact HMIS Lead staff when a duplicate client had been added accidentally and HMIS staff will merge clients.

Policy 10.3.2: All HMIS Member Agency client data should adhere to HMIS capitalization guidelines.

Procedure: HMIS Member Agencies are trained on the current method and style to enter client level data. No HMIS Member Agency should enter a client in any of the following ways:

- ALL CAPS
- all lower case
- Mix OF loWEr and UPPER cAse lEtters
- Enter nicknames in the name space (please use the Alias box).

Policy 10.4: The Homeless Management Information System staff will evaluate the quality of all HMIS Member Agency data on the timeliness of the data entered.

Procedure: Timeliness is an important measure to evaluate daily bed utilization rates and current client system trends. To ensure reports are accurate, Member Agencies should ensure that their internal processes facilitate real-time data entry.

Policy 10.4.1: All HMIS Member Agency client data should be entered in real-time or no later than 24 hours after intake, assessment, or program or service entry or exit.

Procedure: Real-time is defined as “the actual time during which a process takes place or an event occurs.” Client data can be entered into HMIS in real-time - as the client is being interviewed at intake or assessment. The more real-time the data, the more collaborative and beneficial client data sharing will be for all HMIS Member Agencies and clients. The goal is to get all program intake and assessment data into HMIS in real-time.

Policy 10.4.2: All HMIS Member Agency providers should backdate any client data not entered in real-time to ensure that the data entered reflects client service provision dates.

Procedure: All required data elements including program entry/exit, service transactions, universal data elements, and bed management must be entered for each client within 24 hours of program entry/exit or service provision dates. If the date was entered more than 24 hours later than the program entry/exit or service provision, the actual data of service or entry/exit must be used.

Policy 10.5: All Homeless Management Information System staff, HMIS Member Agency providers, and data partners will work together to ensure the highest quality of data in HMIS.

Procedure: Due to the many reports the HMIS staff is asked to provide, HMIS Member Agencies' response to HMIS staff inquiries and correction of data quality issues is critical. Many of our project partners have very rigid time frames in which the HMIS staff must provide updated information. Therefore, the Member Agency will provide a designated Agency Administrator whose role is to communicate with HMIS staff regarding these issues and ensure that the following measures are met.

Policy 10.5.1: All Agency Administrators should respond to HMIS staff inquiries no later than 24 business hours.

Procedure: The Agency Administrator or backup Agency Administrator should respond to inquiries from HMIS staff no later than 24 business hours. In instances of vacation or illness, the back-up Agency Administrator will be contacted.

Policy 10.5.2: All HMIS Member Agency providers should correct client data in HMIS within 5 business days of notification of data errors.

Procedure: After a report that outlines data corrections has been sent to the HMIS Agency Administrator or backup Agency Administrator, it is the responsibility of the Member Agency to correct the issues within 5 business days. Once the corrections have been made, the Agency Administrator or backup Agency Administrator should update the HMIS staff.

Policy 10.6: All Homeless Management Information System staff, HMIS Member Agency providers, and data partners will work together to ensure accuracy of reporting.

Procedure: The HMIS software includes a series of reports to aid in outcome evaluation, data quality monitoring, and analysis of system trends.

Policy 10.6.3: The Homeless Management Information System staff may provide specialty reports to all HMIS Member Agency providers for a fee.

Procedure: Assistance from the HMIS staff to customize reports may be a fee-based service. A request must be submitted to the HMIS staff for evaluation and fee determination.

Section 11: Performance Measurement

HMIS staff will measure the performance of HMIS Member Agency providers as it relates to the quality of the data entered into the system. Additionally, performance on a system-level will be measured to show the progress towards our Continuum of Care in ending homelessness.

Policy 11.1: HMIS staff will measure the timeliness and completeness of data entered by each HMIS Member Agency.

Procedure: As a quality monitoring tool, the HMIS staff will measure the effectiveness of data entry performed by each HMIS Member Agency. These reports will be generated out of the system on a monthly basis. Each HMIS Member Agency will have 5 business days to seek technical assistance regarding and/or correct any data quality issues.

Policy 11.2: HMIS staff will measure the bed utilization rates of homeless housing providers.

Procedure: As a quality monitoring tool, the HMIS staff will periodically review the bed utilization rates of HMIS Member Agencies.

SIGNATURE PAGE

As a partnering Agency/Organization/Project in the Knoxville-Knox County Homeless Management Information System (KnoxHMIS), you authorized and accept responsibility for reading the KnoxHMIS HUD mandated policies, plans, other instructional information provided to you, and will ensure that all personnel with access to HMIS will also accept responsibility for familiarizing his/herself with this information.

In signing this document, you're stating that you are knowledgeable of KnoxHMIS requirements and have access to the following from KnoxHMIS Manager/System Administrator II:

1. KnoxHMIS User Policy Agreement*
2. KnoxHMIS Policies & Procedures**
3. KnoxHMIS Notice of Uses and Disclosures**
4. KnoxHMIS Formal Grievance*
5. KnoxHMIS Partner Projects Listing**
6. KnoxHMIS Data Quality And Monitoring Plan**
7. KnoxHMIS Project Privacy Plan**
8. Business Associate Agreement**
9. Agency Partner Agreement**

*indicates includes in the Apendix

**indicates can be found on our website: www.knoxhmis.org

Agency/Program Staff

Date Signed

KnoxHMIS Administrator Staff

Date Signed

APPENDIX

User Policy, Responsibility Statement & Code of Ethics, page 1 of 2

For: _____ from: _____
User Name (*print Name*) Agency Name (*print Name*)

USER POLICY

Partner Agencies who use the Knoxville HMIS and each User within any Partner Agency is bound by various restrictions regarding the Client information.

It is a Client's decision about which information, if any, is entered into HMIS and whether that information is to be shared and with any Partner Agencies. **Client Consent/Release of Information** shall be signed by Client before any identifiable Client information is entered into HMIS or designated in HMIS for sharing with any Partner Agencies. User shall insure that prior to obtaining Client's signature; the Knoxville HMIS **Notice to Clients of Uses and Disclosures** was fully reviewed with Client in a manner to insure that Client fully understood the information (e.g. securing a translator if necessary).

USER CODE OF ETHICS

Users must be prepared to answer Client questions regarding HMIS.

Users must faithfully respect Client preferences with regard to the entry and sharing of Client information within HMIS. Users must accurately record Client's preferences by making the proper designations as to sharing of Client information and/or any restrictions on the sharing of Client information.

Users must allow Client to change his or her information sharing preferences at the Client's request.

Users must not decline services to a Client or potential Client if that person refuses to allow entry of information into HMIS or to share their personal information with other agencies via HMIS.

The User has primary responsibility for information entered by the User. Information Users enter must be truthful, accurate and complete to the best of User's knowledge.

Users will not solicit from or enter information about Clients into HMIS unless the information is required for a legitimate business purpose such as to provide services to the Client.

Users will not alter or over-write information entered by another Agency.

Users will not use HMIS database for any violation of any law, to defraud any entity or conduct any illegal activity.

Upon Client written request, users must allow a Client to inspect and obtain a copy of the Client's own information maintained within HMIS. Information compiled in reasonable anticipation of or for use in a civil, criminal or administrative action or proceeding need not be provided to Client.

Users must permit Clients to file a written complaint regarding the use or treatment of their information within HMIS. Client may file a written complaint with either the Agency or Knoxville HMIS at The University of Tennessee College of Social Work, 1618 Cumberland Ave. Knoxville, TN 37996. Client may not be retaliated against for filing a complaint.

USER RESPONSIBILITY

Your username and password give you access to the HMIS software. Users are also responsible for obtaining and maintaining their own security certificates in accordance with Agency Partner Agreement.

User Policy, Responsibility Statement & Code of Ethics, page 2 of 2

Initial each item below to indicate your understanding and acceptance of the proper use of your username and password. Failure to uphold the confidentiality standards set forth below is grounds for immediate termination from HMIS database access, and may result in disciplinary action from the Partner Agency as defined in the Partner Agency's personnel policies.

I agree to maintain the confidentiality of Client information in HMIS in the following manner:

- My username and password are for my use only and will not be shared with anyone.
- I will not use the browser capacity to remember passwords: I will enter the password each time I log on to the HMIS.
- I will take reasonable means to keep my password physically secure.
- I will only view, obtain, disclose, or use the database information that is necessary to perform my job.
- I understand that the only individuals who may directly access HMIS Client information are authorized users, and I will take these steps to prevent casual observers from seeing or hearing HMIS Client information.
- I will log off of HMIS before leaving my work area, or make sure that the HMIS database has "timed out" before leaving my work area.
- I will not leave unattended any computer that has HMIS "open and running".
- I will keep my computer monitor positioned so that persons not authorized to use HMIS cannot view it.
- I will store hard copies of HMIS information in a secure file and not leave such hard copy information in public view on my desk, or on a photocopier, printer or fax machine.
- I will properly destroy hard copies of HMIS information when they are no longer needed unless they are required to be retained in accordance with applicable law.
- I will not discuss HMIS confidential Client information with staff, Clients, or Client family members in a public area.
- I will not discuss HMIS confidential Client information on the telephone in any areas where the public might overhear my conversation.
- I will not leave messages on my agency's answering machine or voicemail system that contains HMIS confidential Client information.
- I will keep answering machine volume low so that HMIS confidential information left by callers is not overheard by the public or unauthorized persons.
- I understand that a failure to follow these security steps appropriately may result in a breach of Client HMIS confidentiality and HMIS security. If such a breach occurs, my access to the HMIS may be terminated and I may be subject to further disciplinary action as defined in the partner agency's personnel policy.
- If I notice or suspect a security breach, I will immediately notify the Director of my Agency and the Knoxville HMIS Security Officer.

I understand and agree to comply with all the statements listed above.

HMIS User Signature		Date		HMIS User Name (<i>please print</i>)
Agency Director Signature		Date		Agency Director Name (<i>please print</i>)
KnoxHMIS Administrator Signature		Date		KnoxHMIS Administrator Name: <i>Print</i>

KnoxHMIS FORMAL GRIEVANCE THIS FORM MUST BE COMPLETELY FILLED OUT

Name of Grievant (Please Print):	Primary Phone: Secondary Phone: E-mail Contact:	
Mailing Address: Street or P.O. Box: City: _____ State: _____ Zip: _____		
Date, time and place of event leading to grievance: _____ Date you notified KnoxHMIS of the event, <i>(if different)</i> : _____		
Detailed description of grievance including names of other persons involved, if any (Grievant): 		
Findings (KnoxHMIS): 		
Proposed solution to grievance (Agency Action Plan): 		
<p><u>Grievant:</u> File a copy of this form with KnoxHMIS and retain a personal copy. This form can be mailed or e-mailed to the following: ATTN: Lisa Higginbotham Program Manager KnoxHMIS Social Work Office of Research and Public Service 600 Henley Street Knoxville, TN 37996-4104 lhigginb@utk.edu</p>		
Grievance Filed With <i>(Please Print Name of KnoxHMIS Staff)</i>	Grievant Signature	Date

KnoxHMIS Office Use Only:

Agency notified? Yes No
 Date Agency Notified: _____ Name of Agency Staff Notified: _____ Title: _____
 KnoxHMIS Policy Provided to Agency: Yes No
 Action Plan provided from Agency to KnoxHMIS? Yes No