Austin / Travis County
Homeless Management Information System (HMIS)

Policies and Procedures Manual

The Austin/Travis County Homeless Management Information System is managed by Ending Community Homelessness Coalition, Inc. (ECHO)

For further information about HMIS contact:

Katy Manganella
HMIS Director
ECHO
300 E. Highland Mall Blvd., Suite 200
Austin TX 78752
(512) 481-2848
katymanganella@austinecho.org

Table of Contents

Introduction

A Homeless Management Information System (HMIS) is a database used to record and track client-level information on the characteristics and service needs of people experiencing homelessness. An HMIS ties together homeless service providers within a community to help create a coordinated and effective housing and service delivery system.

The U.S. Department of Housing and Urban Development (HUD) and other planners and policy-makers at the federal, state, and local levels use aggregate HMIS data to obtain better information about the extent and nature of homelessness over time. Specifically, an HMIS can be used to produce an unduplicated count of people experiencing homelessness, understand patterns of needs and service use, and measure the effectiveness of homeless programs and systems.

Austin / Travis County's HMIS is led by the Ending Community Homelessness Coalition (ECHO). The HMIS staff are responsible for the local administration of the HMIS software and they provide technical assistance to participating agencies and end users.

Agencies that participate in the Austin / Travis County HMIS are referred to as "participating agencies." Each participating agency needs to follow certain guidelines to help maintain data privacy and accuracy.

History

In 2001, Congress instructed the U.S. Department of Housing and Urban Development (HUD) to take measures to improve available data concerning homelessness in the United States. In response, HUD mandated all Continuum of Care (CoC) regions to implement CoC-wide databases that would allow an unduplicated count of clients served, information about their needs, program participation, and outcomes of services provided. Out of this directive came the Homeless Management Information System (HMIS), an electronic data collection application that facilitates the collection of information on individuals and families experiencing homelessness who access homeless assistance service agencies and stores that data in a centralized database.

Why is this important?

Using a centralized database, HMIS, is advantageous for both service providers and the clients in need of assistance to end their homelessness. The HMIS software used in Austin / Travis County allows client data sharing between organizations, as well as client case coordination and electronic referrals. The information-sharing model can prevent service duplication and enable collaboration between multiple homeless service providers, while limiting access to sensitive data and protecting private client information.

In addition to standard data collection and reporting functionality, the HMIS software includes a comprehensive case management module, bed management, performance

measurement tools, functionality for customized reporting, and software customization options.

Lastly, HMIS participating agencies are better positioned for future funding opportunities. Many national and local funders require HMIS participation for homeless service programs. Participating agencies and the people they serve benefit from a community-wide response to homelessness in addition to their organizational response.

Roles and Responsibilities

The Ending Community Homelessness Coalition (ECHO) holds a HMIS Memorandum of Understanding (MOU) with each participating agency. The MOU outlines the roles and responsibilities of ECHO, as the HMIS-Lead Agency, and the participating agency.

The responsibilities of each party, described further throughout this Manual, are summarized here for ease of reference:

Ending Community Homelessness Coalition (ECHO) Responsibilities

- Execute HMIS Memorandums of Understanding with each participating agency
- Contract with Mediware Information Systems and locally administrate the local HMIS software system
- Oversee all HMIS access, including end user licensing and PKI (Public Key Infrastructure) certificates
- Provide training and technical support to participating agency end users
- Conduct training and HMIS implementation in a way that respects the privacy and dignity of the people whose data is collected
- Oversee safety and privacy of HMIS data
- Monitor data quality and compliance with applicable HMIS standards at least monthly
- Execute End User Agreements with each end user
- Develop and update as needed all HMIS policies and procedures
- Facilitate the HMIS Workgroup
- Review national, state, and local laws that govern privacy or confidentiality protections and make determinations regarding relevancy to existing HMIS policies
- Provide New User Training, Ethics Refresher Training, Agency Admin Training, and Reporting Training on a regular basis
- Oversee and submit to the U.S. Department of Housing and Urban Development all CoC-level HMIS reports including the Point in Time Count report, Housing Inventory Count report, Annual Homeless Assessment Report, and System Performance Measure Reports
- Coordinate software enhancement implementations with the software vendor, Mediware Information Systems

Participating Agency Responsibilities

- Comply with all applicable agreements, including all appendices in this Manual.
- Comply with the HUD HMIS Data Standards
- Uphold HMIS data quality by accurately entering all required data into the HMIS system, as described in the HMIS Data Quality Assurance Plan
- Identify and appoint a HMIS Agency Administrator as the primary point of contact for all HMIS activities at the agency. Responsibilities of the Agency Administrator are described in the HMIS Agency Administrator Agreement.
- Pay annual HMIS licensing fees to ECHO upon receipt of invoice.
- Oversee all agency staff that generate or have access to client-level data stored in the HMIS and ensure adherence to all applicable privacy policies and regulations.
- Holds final responsibility for the adherence of the agency's personnel to the Privacy, HIPAA, and all State and Federal laws and regulations, as well as ensures adherence to the HMIS policies and procedures outlined in this document.
- Responsible for all activity associated with staff access and use of the HMIS consistent with this document
- Assume protection of client-level data entered into and accessed in the HMIS system at the agency
- Ensure that data is collected in a way that respects the dignity of participants
- Ensure that all data collected is relevant to the purpose for which it is used
- Ensure that the Privacy Notice is posted in any space where HMIS data is collected and provide a copy of the notice to clients upon request
- Provide prompt and timely communications of data concerns and/or emergencies, changes to end user staffing, user accounts, and software to ECHO HMIS staff.
- Maintain and dispose of on-site computer equipment and data used for participation in HMIS
- Deactivate HMIS end user accounts within 24 hours after the end user no longer needs HMIS access or has left the organization.
- Notify the HMIS Director in writing of any audit notices, legal matters, and research that may require data from HMIS to be released.
- Submit monthly HMIS data quality reports to ECHO on time
- Ensure the Agency Administer represents the agency at the HMIS Workgroup Meeting
- Work collaboratively with ECHO to ensure accuracy of data and project settings in HMIS for all applicable federal reports on behalf of the Continuum of Care
- Collect and enter HMIS data into the HMIS system for all Agency programs that are active in HMIS.

HMIS Workgroup Member Responsibilities

The purpose of the HMIS Workgroup is governance over the HMIS requirements. Each participating agency's Agency Administrator is a member of this body. The HMIS Workgroup reports to the HUD Continuum of Care (CoC) and Emergency Solutions Grant (ESG) Committee, which reports to the CoC Membership Council.

HMIS Workgroup Responsibilities

- Informs and reviews changes to all HMIS policies and leads implementation within their agency
- Informs and reviews changes to the HMIS Data Sharing Policy and Release of Information (ROI) for HMIS client data sharing
- Understands and implements changes from the HUD HMIS Data Standards
- Reviews local reports to HUD ensure accuracy, including the Point in Time Count Report, Housing Inventory Count Report, Annual Homeless Assessment Report, and the System Performance Measure Reports
- Provides feedback to ECHO HMIS staff for continuous quality improvement

Implementation Policies and Procedures

HMIS Memorandum of Understanding (MOU)

The Executive Director, or equivalent, of each participating agency shall follow, comply, and enforce the HMIS Memorandum of Understanding (MOU). The Executive Director / equivalent must sign the HMIS MOU before the agency is granted access to HMIS. Signing the HMIS MOU is a precursor to training and end user access.

1. The signed HMIS MOU must be presented to the ECHO HMIS Director before any end user at the agency is granted access to the HMIS.
2. After the HMIS MOU is signed, ECHO will invoice the participating agency for intended HMIS user licenses.
3. The participating agency is responsible for submitting payment upon receipt of this invoice.
4. Then, the HMIS staff can proceed with training new end users and granting access to the HMIS.

HMIS User Agreement

Each end user of any participating agency shall follow, comply, and enforce the HMIS User Agreement. Before given access to HMIS, the end user must sign a HMIS User Agreement.

1. The HMIS staff will provide the end user a HMIS User Agreement for signature after completing required training.
2. The HMIS staff will collect and maintain HMIS User Agreements for all end users.
3. A copy of the HMIS User Agreement will be given to each end user for their records.

HMIS Agency Administrator Agreement

Each participating agency's Executive Director, or equivalent, will designate one HMIS user as the Agency Administrator, who holds responsibility for data security at the agency and coordination of the HMIS at the agency.

1. The Agency Administrator will attend Agency Administrator Training.
2. The HMIS staff will provide the Agency Administrator a HMIS Agency Administrator and Data Security Officer Authorization Form for signature after completing training.
3. Both the Agency Administrator and the participating agency's Executive Director, or equivalent, will sign the Agreement and return it to ECHO HMIS.
4. HMIS staff will set the Agency Administrator's access level in HMIS.
5. The HMIS staff will maintain record of Agency Administrator Agreements and will grant Agency Administrator access in the HMIS.

Data Collection Requirements

The U.S. Department of Housing and Urban Development (HUD) identifies the core data elements that are required for collection in the HMIS Data Standards Manual. HUD maintains this manual and revises as necessary.

At a minimum, all participating agencies collect and enter the Universal Data Elements and applicable Program-Specific Data Elements. In some cases, HMIS programs collect locally agreed upon data elements in addition to the minimum requirements from HUD. Participating agencies should consult with ECHO HMIS to determine which elements apply to their programs in HMIS.

In some cases, participating agencies have data collection requirements beyond what HUD outlines in the HMIS Data Standards Manual. These requirements usually come from other federal partner and local program funders. In these cases, the participating agency will consult with ECHO HMIS during initial program set up in HMIS, or when changes occur, to ensure all required elements are incorporated.

Participating agencies will collect and enter in HMIS the minimum set of data elements for all clients served by their programs within the timeline outlined in the HMIS Data Quality Assurance Plan.

HMIS Technical Support Protocol

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

1. HMIS end users should first seek technical support from their HMIS Agency Administrator.
2. If more support is needed, the Agency Administrator or the end user should submit a HMIS Help Desk Ticket to ECHO.
3. Technical support hours are Monday through Friday (excluding holidays) from 9:00 AM – 5:00 PM.

4. The HMIS staff strive to respond to all HMIS Help Desk Tickets within 2 business days of receipt and typically have same-day response turnaround. ECHO will communicate to the end user when the ticket will require more than 48 business hours to resolve.

The participating agency is responsible for troubleshooting problems with HMIS access due to internet connection at their agency.

HMIS Licenses and Support Protocol

The Austin/Travis County CoC purchases HMIS licenses from ECHO. The license fee covers the license charges from the software vendor and a reasonable amount of support from ECHO throughout the 12-month billing cycle. The HMIS billing cycle begins March 1 and ends on February 28/29 the following year (e.g. The 2018-19 billing cycle is March 1, 2018 – February 28, 2019). HMIS access and support are included with each license.

Refer to the HMIS License and Support document for more information regarding licensing fees.

Process for renewing licenses at beginning of billing cycle:

1. ECHO will confirm with each participating agency at the end of the billing cycle if they intend to participate in HMIS in the following billing cycle.
2. ECHO will confirm the number of licenses the participating agency is using and intends to use in the next billing cycle.
3. ECHO will send an invoice for the specific number of licenses intended for use in the next billing cycle to the participating agency.
4. The participating agency is responsible for submitting payment upon receipt of this invoice.
5. Once paid for, the licenses remain available to the participating agency through the remainder of the billing cycle.

If the participating agency does not intend to participate in HMIS in the next billing cycle, the licenses used by that agency will expire at the end of the current billing cycle.

Process for purchasing additional licenses during the billing cycle:

1. The participating agency will inform the HMIS Director that they want to purchase additional licenses after the current billing cycle has started.
2. The HMIS Director will confirm the number of additional licenses needed and when the additional licenses need to be available for use.
3. The HMIS Director will work with the ECHO Chief Financial Officer to prorate the additional licenses for the remainder of the billing cycle.
4. ECHO will send an invoice for the additional license(s) to the participating agency.
5. The participating agency is responsible for submitting payment upon receipt of invoice.

6. Once paid for, the licenses remain available to the participating agency through the remainder of the billing cycle and are eligible for renewal at the end of the cycle.

Process for returning licenses purchased:

1. There are no returns on HMIS licenses purchased by a participating agency. In other words, if a participating agency decides they do not want a license they purchased for the billing cycle, ECHO is unable to refund the cost of the license to the participating agency.
2. The license will remain available to the participating agency throughout the duration of the billing cycle.
3. The participating agency will have the opportunity not to renew any unused licenses at the end of the current billing cycle.

Process for transferring licenses between participating agency staff:

1. An HMIS license can only be attached to one end user account at a time.
2. As described in this Manual, the participating agency has discretion over which staff require an HMIS license and HMIS access for their role.
3. After receiving the proper HMIS training, an HMIS license can be transferred from one end user to another end user at the same participating agency in HMIS.
4. When a license is transferred, the end user initially holding the license will lose access to HMIS.
5. ECHO will work closely with the participating agency to ensure the timing of the transfer is appropriate.
6. ECHO is responsible for transferring the license between end user accounts to maintain security of the system.

Security Policies and Procedures

Training

HMIS staff facilitate ongoing training for HMIS end users and agency administrators. The training schedule is published on the ECHO website.

Training Type	Course Detail	Requirements
New User Training	Users learn the basic skills and concepts needed for HMIS data entry. This includes: Standard operating procedures, privacy and client consent, ethics, software features, system security, and an introduction to the Continuum of Care	Once for all end users
Ethics Refresher Training	Refreshes the skills of active users and reviews ethics, privacy, and client consent policies and procedures	Annually for all end users

Reporting Training	Users with reporting licenses are given an overview of the various reporting options available and how to use them	Encouraged for anyone using reporting functionality
Agency Administrator Training	Agency Administrators are trained on roles and responsibilities, system administration, system security, and providing HMIS support to end users at their agency	All HMIS Agency Administrators

User Authentication and Access

Only users with a valid username and password can access HMIS. The Agency Administrator will provide a unique username and initial password for the end user after completion of required training and signing the HMIS User Agreement.

1. The participating agency will determine which of their employees will be HMIS end users. User access will be granted only to those individuals whose job functions require legitimate access to the system.
2. Proposed end user will complete the required training and demonstrate proficiency in use of the system.
3. Proposed end user will sign the HMIS User Agreement stating that they have completed training, will abide by the Policies and Procedures, will uphold privacy and confidentiality of client information accordingly, and will only collect, enter and retrieve data in the system relevant to the delivery of services to people.
4. The HMIS staff will be responsible for the distribution, collection, and storage of the signed HMIS User Agreements.
5. The Agency Administrator will set up the new user in HMIS, including setting the username and initial password.
6. The HMIS staff will then assign a HMIS license to the user's account and install a PKI certificate on the user's computer so they are able to access the HMIS site.
7. Sharing of usernames and passwords is a breach of the HMIS User Agreement.
8. When an end user leaves employment or no longer needs access to HMIS, the Agency Administrator will de-activate the end user's HMIS account and will notify the HMIS staff.
9. HMIS staff will remove the license and remove the user's account.

After an end user no longer needs HMIS access or has left the organization, their HMIS account must be deactivated and deleted:

1. The Agency Administrator is responsible for deactivating end user accounts in a timely manner, within 24 hours, after the end user no longer needs HMIS access.
2. After deactivating, the Agency Administrator is responsible for informing the ECHO HMIS staff that the end user is no longer active.
3. The HMIS Director, or designee, is responsible for deleting the end user's account from HMIS. This will make the user license attached previously to that account available for reassignment to a replacement staff.

PKI Security Certificate

All computers and each individual end user account on each computer that accesses HMIS must have a current PKI Security Certificate installed in order to access the HMIS login screen. The HMIS staff will install the appropriate PKI Security Certificate as required and the following conditions are met:

1. The end user has received and completed all required HMIS trainings.
2. The end user has signed the HMIS End User Agreement.
3. The end user has submitted an HMIS Help Desk Ticket requesting the PKI installation on their computer.
4. The PKI Security Certificate can only be installed on computer equipment owned and supplied by the participating agency. Otherwise stated, the PKI Security Certificate cannot be installed on an end user's personal computer or device.

Participating agencies and users cannot ask for or take possession of the PKI installation software. HMIS staff will not offer or provide the PKI installation software to anyone except for other HMIS staff.

Passwords

Each end user will have access to HMIS via a username and password. Passwords will expire every 45 days and must be updated at that time by the end user. End users will maintain password confidentiality. End users are strictly prohibited from storing or displaying any information pertaining to user access (e.g. username and password).

1. The Agency Administrator will set up the end user in HMIS, including setting the username and initial password.
2. The initial password is a temporary password and will expire the first time the end user logs into their account, requiring that they change their password.
3. The end user will be required to create a permanent password that is 8-50 characters long with at least two numbers or symbols.
4. End users may not use the same password consecutively but may use the same password more than once.
5. Access permission will be removed after the end user unsuccessfully attempts to log in three times. The end user will be unable to gain access until the HMIS staff or their Agency Administrator reset their password.
6. To request that HMIS staff reset their password, the end user should submit a HMIS Help Desk Ticket to ECHO.

Hardware Security Measures

Computer Equipment: The participating agency is responsible for maintenance of each end user's computer equipment used to access HMIS. All computers and networks used to access HMIS must have virus protection software and firewall installed. Virus definitions and firewall must be regularly updated. Only computer equipment belonging

to and supplied by the participating agency can access HMIS. In other words, end user personal computers are strictly prohibited from accessing HMIS.

The federal regulations state that: Physical access to systems with access to HMIS data computers that are used to collect and store HMIS data will be staffed at all times when in public areas. When workstations are not in use and staff are not present, steps will be taken to ensure that the computers and data are secure and not publicly accessible. These steps must minimally include:

1. Logging out of HMIS.
2. Logging out of the computer with password protection.

Internet Connection: The participating agency is responsible for troubleshooting problems with HMIS access due to internet connection.

Data Retention and Disposal

Paper Records: ECHO does not require the retention of paper copies or hard copies of any HMIS records.

ECHO understands, however, that participating agencies may have requirements for keeping paper records containing HMIS data. Participating agencies agree to follow their existing policies and procedures and applicable local, state, and federal laws and regulations for access to HMIS client records stored on paper. All paper or other hard copy files containing Protected Personal Information (PPI) must be directly supervised when the hard copy is in a public area. If agency staff are not present, the information must be secured in areas that are not publicly accessible.

Electronic Records: If the participating agency needs to download Protected Personal Information (PPI) from HMIS, the participating agency is responsible for ensuring the protection of this confidential information. Once PPI has been downloaded from HMIS to an agency's computer, the security of this data becomes the responsibility of the agency.

At a minimum, the participating agencies agrees to the following as it pertains to all forms of HMIS data retention and disposal:

1. The participating agency agrees to only keep copies of files containing HMIS PPI for clearly definable reasons, including statutory, regulatory, contractual, or other requirements mandating retention of HMIS records including PPI.
2. All computers that have HMIS PPI saved locally must be password protected to login.
3. The participating agency agrees to dispose of all documents and files containing HMIS PPI in a manner that will protect client confidentiality. Methods include:
    a. Shredding applicable paper records
    b. Deleting any information from computers and destroying the files before disposal

c. Triple formatting hard drives of any machine containing PPI before transfer of property and/or destruction of hard drives of any machine that has contained HMIS PPI before disposal

4. PPI saved in locations outside of HMIS that is not in current use seven years after the PPI was created or last changed must be deleted unless a statutory, regulatory, contractual, or other requirement mandates longer retention. Care must be taken to assure that the guidelines associated with data disposal are properly followed.

Security Review

HMIS staff will complete an annual review to ensure the implantation of the HMIS Privacy and Security Plan requirements for itself and participating agencies. The security review will include the completion of the HMIS Privacy and Security Assessment Form ensuring that each security standard is implemented.

Security Violations and Sanctions

Any end user found to be in violation of security protocols of their agency's procedures or HMIS Policies and Procedures will be sanctioned accordingly. All end users must report potential violation of any security protocols to ECHO.

1. End users are obligated to report suspected instances of noncompliance and/or security violations immediately to the ECHO HMIS Director.
2. The participating agency is obligated to help ECHO investigate potential HMIS violations.
3. Any end user found to be in violation of security protocols will be sanctioned accordingly. Sanctions may include but are not limited to suspension of system privileges, attending additional training, and revocation of system privileges.
4. In the case of pervasive or severe violations of security protocols by a participating agency, ECHO can revoke or suspend system access and participation to the entire agency.

Client Consent Procedure for HMIS Data Sharing

Client informed consent of data sharing within HMIS must be documented for each participating agency that serves the client. This includes notice that client data will be entered into the HMIS system and a Data Sharing Policy and Release of Information (ROI) for sharing client data must be on file for each client.

Each HMIS participating agency must publish a privacy notice describing its policies and practices for the processing of client data and must provide a copy of its privacy notice and HMIS Privacy Policy Statement to any individual upon request. The HMIS Lead Agency, ECHO, maintains a copy of the HMIS Privacy Notice and the full HMIS Privacy Policy Statement on the ECHO website: www.austinecho.org

The HUD HMIS Data and Technical Standards require that each HMIS participating agency post the Privacy Notice at each intake desk or comparable location where HMIS data is collected. The notice explains generally the reasons for collecting protected personal information (PPI). PPI is defined by HUD as “any information maintained by or for a Covered Homeless Organization about a living homeless client or homeless individual that: 1) Identifies, either directly or indirectly, a specific individual; 2) can be manipulated by a reasonably foreseeable method to identify a specific individual; or 3) can be linked with other available information to identify a specific individual.”

Each HMIS participating agency must specify on its privacy notice the purposes for which it collects client data and must describe all uses and disclosures. A participating agency may use or disclose client data only if the use or disclosure is allowed by this standard and is described in its privacy notice.

Each participating agency must allow clients they serve to have a copy of any data about themselves in HMIS, upon request. The participating agency must offer to explain any information that the client may not understand. Participating agencies must consider any request by a client for correction of inaccurate or incomplete data pertaining to themselves in HMIS. The participating agency is not required to remove any information, but should alternatively choose to update information, mark it as inaccurate, or incomplete, and should supplement it with additional information.

Inter-Agency Data Sharing Agreement

The Austin / Travis County HMIS promotes the coordinated assessment, intake and referral process to better serve clients. We accomplish this by sharing authorized client information through an Inter-Agency Sharing Agreement.

1. ECHO HMIS and each participating agency will comply with all applicable federal and state laws regarding the protection of client privacy.
2. The participating agency acknowledges and understands that the Austin / Travis County HMIS shares all authorized client information with every other participating agency within HMIS. The data is identified through the HMIS Data Sharing Policy and Release of Information (ROI).
3. The participating agency, by signing the HMIS Memorandum of Understanding (MOU) which includes this document, hereby enters into an Inter-Agency Data Sharing Agreement.
4. The participating agency acknowledges that in transmitting, receiving, storing, processing or otherwise dealing with any client protected information, they are fully bound by federal and state regulations governing confidentiality of patient records **where applicable**, including the Federal Law of Confidentiality for Alcohol and Drug Abuse Patients (42 CFR Part 2), and the Health Insurance Portability and Accountability Act of 1996 (HIPAA, 45 CFR Parts 160 & 164), and cannot use or disclose the applicable information except as permitted or required by this agreement or law.

5. The participating agency acknowledges that they are prohibited from making any further disclosure of HMIIS information unless that disclosure is expressly permitted by the written consent of the person to whom it pertains or as otherwise permitted or required by state and federal regulations governing confidentiality of records, including the Federal Law of Confidentiality for Alcohol and Drug Abuse Patients (42 CFR Part 2), and the Health Insurance Portability and Accountability Act of 1996 (HIPAA, 45 CFR Parts 160 & 164).
6. The participating agency agrees to notify ECHO, within one business day, of any breach, use, or disclosure of information not provided for by this agreement.
7. The participating agency acknowledges that the participating agency, itself, bears primary responsibility for oversight for all sharing of data collected and entered HMIS.

Confidentiality and Informed Consent

Each client must provide informed consent, which includes both an oral explanation and written client consent, for sharing information within HMIS and outside of HMIS.

Oral explanation: The participating agency will provide all clients with an oral explanation of the HMIS and terms of consent, per the HMIS Data Sharing Policy and Release of Information (ROI). The agency is responsible for ensuring that this procedure takes place prior to every intake interview. The oral explanation must contain the following information, as further described in the HMIS Data Sharing Policy and Release of Information (ROI):

1. What the HMIS is:
    a. A computer-based information system that organizations that provide services to end homelessness in Austin / Travis County use to capture information about the people they are providing services to and the outcomes of those services.

2. Why the agency uses it:
    a. To understand and better meet their client's needs
    b. Help the organization plan for their programs to have appropriate resources for the people they serve
    c. To understand the outcomes of the services the organization provides
    d. To inform public policy to end homelessness

3. Security
    a. Only staff who work directly with clients or who have administrative responsibilities have access to HMIS, including the ability to look at, enter, and edit client records

4. Privacy Protection
    a. Basic information will be shared with all HMIS participating agencies

b. Clients have the right to not answer any question, unless that answer is needed to know if the program is able to work with the client (determine and document eligibility)
c. Clients have the right to know who has added to, deleted, or edited their HMIS client record
d. Information that is transferred over the internet is through a secure connection and/or is de-identified

5. Benefits for clients
    a. Case manager and client can use information to assist clients with obtaining resources that will end their homelessness
    b. Case managers working with the client at different participating agencies can collaborate to better serve the client
    c. Client has a record of the organizations and programs they have worked with and documentation of their homelessness, which can be used for program eligibility documentation

Written client consent: A client must be informed what information is being shared, with whom it is being shared, and the expiration date of the consent. A client must sign a consent form, called the HMIS Data Sharing Policy and Release of Information (ROI), authorizing information sharing outside of HMIS. The Data Sharing Policy and ROI must be uploaded to the client's HMIS profile as documentation of their consent and sharing choice. Clients can change their consent and sharing choice at any time, per the HMIS Data Sharing Policy and ROI.

Data Policies and Procedures

Data Quality

All data entered into HMIS must meet data quality standards. Participating agencies will be responsible for their users' quality of data entry. Data quality standards are described in detail in the Data Quality Assurance Plan and summarized here.

Definition:
Data quality refers to the timelessness, completeness, and accuracy of information collected and reported in the HMIS.

Data Timeliness:
End users must enter all HMIS data into HMIS within 5 business days of collecting the HMIS data. This applies to all data collection points, including updates.

Data Completeness:
All data entered into HMIS is complete.

Data Accuracy:

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

- Participating agencies must sign the HMIS Memorandum of Understanding (MOU) to ensure that all participating programs are aware and have agreed to the data quality standards.
- Upon agreement, participating agencies will collect and enter as much relevant client data as possible for the purposes of providing services to that client.
- All data will be input into the system no more than 5 business days after it is collected.
- All HMIS Agency Administrators will conduct monthly checks for data quality. Data quality reports will be submitted to ECHO monthly, including any patterns of error or missing data.
- End users will be required to correct any identified data errors and will be monitored for compliance by the participating agency and the HMIS staff.
- End users may be required to attend additional training as needed.
- In the case of egregious and repeated data quality errors, ECHO can suspend or revoke HMIS access to the end user.

Data Use and Disclosure

All end users will follow the Data Use and Disclosure Policies and Procedures to guide the data use of client information stored in HMIS.

Client data may be used or disclosed for system administration, technical support, program compliance, analytical use, and other purposes as required by law. Use involve sharing parts of client information with staff within a participating agency. Disclosures involve sharing parts of client information with staff or organizations outside of the participating agency.

Participating agencies may use data contained in the system to support the delivery of services to clients in the continuum. Agencies may use client information internally for administrative functions, technical support, and management purposes. Participating agencies may also use client information for internal program analysis, such as analyzing client outcomes to evaluate program effectiveness.

Data Release

All HMIS participating agencies and stakeholders will follow the data release Policies and Procedures to guide the data release of client information stored in HMIS.

Data release refers to the dissemination of aggregate or anonymous client-level data for the purposes of system administration, technical support, program compliance, and analytical use.

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

- Aggregate data may be released without agency permission at the discretion of the Continuum or Lead Agency. It may not release any personal identifiable client data to any group or individual without written permission from the client.

- The participating agency will uphold federal and state confidentiality regulations to protect client records and privacy. In addition, the participating agency will only release client records with written consent by the client, unless provided for in the regulations.

Data Release During an Audit

ECHO must be notified if a participating agency is required to release data from HMIS during an audit.

1. Participating agency receives an audit notice.
2. Participating agency contacts HMIS Director in writing to notify ECHO that HMIS data may be released.
3. ECHO may request a copy of the audit notice from the participating agency and may seek legal counsel.
4. ECHO and participating agency will collaborate to ensure only the data required to be released during the audit is released.

If ECHO is audited, ECHO will notify the relevant participating agencies.

1. ECHO receives an audit notice.
2. ECHO will determine which data is required for release and may seek legal counsel.
3. ECHO must release data in accordance with the audit.
4. ECHO will notify all relevant participating agencies in writing of the audit.

Data Release for Research

Participating Agencies in HMIS collect personal client information only when appropriate to provide services or for other specific purposes of the organization or when required by law. The HMIS Lead Agency will review and respond to requests for the use of HMIS data for research.

Purposes for which agencies collect protected personal information may include the following:

- Provide or coordinate services to clients
- Locate other programs that may be able to assist clients
- Functions related to payment or reimbursement from others for services that we provide

- Operate the agency, including administrative functions such as legal, audits, personnel, oversight, and management functions
- Comply with government reporting obligations
- When required by law
- For research purposes

HMIS Release of Data for Research Conditions:

- No client protected personal information for any reason may be released to unauthorized entities
- Only de-identified aggregate data will be released, unless the client consents to sharing their identifiable information
- Parameters of the aggregate data, that is, where the data comes from and what it includes will be presented with each release
- Research results will be reported to the HMIS Lead Agency prior to publication, for publication approval by the HMIS Lead Agency
- Research will be shared with the participating agencies after publication
- HMIS Lead Agency will be granted the rights to utilize all findings (results).

Inclusion in HMIS Federal Reporting

ECHO, as the HMIS Lead Agency for Austin/Travis County, is required by the U.S. Department of Housing and Urban Development to participate in HMIS federal reporting on behalf of the Austin / Travis County Continuum of Care (CoC) for Austin / Travis County to receive federal funding for ending homelessness.

By participating in HMIS, the participating agency acknowledges and understands that data entered in HMIS for their programs may be included in applicable and required federal reporting.

Report Name	**Project Types Included**
Point in Time Count Sheltered Report	1. Emergency Shelters 2. Transitional Housing 3. Safe Havens
Housing Inventory Count Report	1. Emergency Shelters 2. Transitional Housing 3. Safe Havens 4. Rapid Rehousing 5. Permanent Supportive Housing 6. Other Permanent Housing
Annual Homeless Assessment Report	1. Emergency Shelters 2. Transitional Housing 3. Permanent Supportive Housing
System Performance Measures	1. Emergency Shelters 2. Transitional Housing

	3. Safe Havens 4. Rapid Rehousing 5. Permanent Supportive Housing 6. Other Permanent Housing 7. Street Outreach

Each participating agency agrees to work collaboratively with ECHO staff to ensure accuracy of data and project settings in HMIS for these reports. Project types included in federal reports on homelessness are subject to change over time in response to HUD requirements.

Questions about HMIS federal reporting should be directed to the HMIS Director.

Appendices

Appendix	Document Title
1	HMIS Memorandum of Understanding (MOU)
2	HMIS Privacy Notice
3	HMIS User Agreement
4	HMIS Agency Administrator Agreement
5	HMIS Data Quality Assurance Plan
6	HMIS License and Support
7	HMIS Privacy and Security Plan
8	HMIS Privacy and Security Assessment Form
9	HMIS Data Sharing Policy and Release of Information (ROI)
10	HMIS Privacy Policy Statement

Appendix 1

Austin / Travis County Homeless Management Information System HMIS Memorandum of Understanding (MOU)

This AGREEMENT is entered into and renewable annually by mutual consent of both parties, Ending Community Homelessness Coalition (ECHO) located at 300 E. Highland Mall Blvd, Suite 200, Austin, TX 78752 and [AGENCY] (AGENCY) located at [ADDRESS].

ECHO is the HMIS lead agency responsible for the management of homeless services in Austin/Travis County. In accordance with the U.S. Department of Housing and Urban Development data collection mandates, ECHO implements and operates a Homeless Management Information System (HMIS) called ServicePoint by Mediware Information Systems for client tracking throughout the Austin/Travis County Continuum of Care.

ECHO and [AGENCY] mutually agree to the following:

- ECHO will allow the AGENCY to utilize ServicePoint (the system), an Internet-based HMIS developed by Mediware Information Systems (MEDIWARE), for the purposes of client tracking and case management for homeless services provided through the agency.
- The AGENCY will collect and enter HMIS data into the HMIS system for all AGENCY programs that are active in the HMIS.
- The AGENCY will purchase licenses for their users at the price outlined in ECHO's HMIS License and Support Policy.
- ECHO will contract with MEDIWARE for the hardware and software services for the HMIS system.
- The AGENCY may not contact MEDIWARE directly and/or request changes from MEDIWARE to the software. All contact and/or requests will be made through ECHO.
- ECHO will maintain control of all data entered into the system and will manage and secure this data in accordance with ECHO's HMIS Privacy Policy and Privacy and Security Plan.
- The AGENCY will comply with the ECHO HMIS Policies and Procedures Manual, the HMIS Privacy Policy and the ECHO HMIS Data Quality Assurance Plan for the use of the system and will designate an Agency Administrator to monitor users for adherence to said policies.
- The AGENCY will be entering into an Inter-Agency Data Sharing Agreement with all active participating agencies in HMIS. The policy is contained within the ECHO HMIS Policies and Procedures Manual.
- Both ECHO and the AGENCY will operate in accordance with HUD's currently published HMIS Data and Technical Standards except in cases where the Standards conflict with Texas law. In such cases, Texas law supersedes the Standards.
- ECHO has the right to terminate this agreement at any time if the ECHO HMIS Policies and Procedures Manual is not followed.
- ECHO is responsible for ensuring that the contract terms of the agreement with MEDIWARE continue to be satisfied so that all agency data remains secure. This responsibility extends to the provision of disaster recovery services, daily backup of data, system maintenance, database level and secure socket layer encryption, and regularly scheduled product upgrades.
- The AGENCY agrees to ensure the designated Agency Administrator's attendance to all HMIS meetings exceeds 50%.

Austin / Travis County Homeless Management Information System
HMIS Memorandum of Understanding (MOU)

The signing of this Memorandum of Understanding certifies concurrence with the terms and conditions agreed upon by both parties hereto; no other agreement, oral or otherwise shall be deemed to exist or be binding.

AGENCY:

Signature and Title of Agency Representative	Date

Ending Community Homelessness Coalition:

HMIS Director Ending Community Homelessness Coalition (ECHO)	Date

Appendix 2

Austin / Travis County Homeless Management Information System
Privacy Notice

This agency collects information about people who ask about our homeless services. When we meet with you, we will ask you for information about you and your family. We will put the information you give us into a computer program called the Austin/Travis County Homeless Management Information System (or "Austin/Travis County HMIS").

We collect personal information directly from you for reasons that are discussed in our Privacy Policy Statement. We may be required to collect some personal information by law or by organizations that give us money to operate this program. Other personal information that we collect is important to run our programs, to improve the services for homeless persons, and to better understand the needs of homeless persons. We only collect information that we consider to be appropriate. In order to provide or coordinate services, we share your information with other organizations that use the Austin/Travis County HMIS system. These organizations are required to have privacy policies in place in order to protect your personal information. You can refuse to answer **any** question at **any** time. You will never be denied help because you didn't answer a question, unless we need that answer to know if you are eligible for a service.

The collection and use of all personal information is guided by strict standards of confidentiality as outlined in our Privacy Policy Statement. A copy of our agency's Privacy Policy Statement is available upon request for your review.

Appendix 3

Austin / Travis County Homeless Management Information System
User Agreement

User (print name) Agency (print name)

User Policy

Partner Agencies who use the Austin / Travis County ServicePoint HMIS system, and each User within any Partner Agency, are bound by various restrictions regarding client information and must comply with HMIS policies and procedures. A User employed at Partner Agencies that are covered entities of the Health Insurance Portability and Accountability Act (HIPAA) have more restrictive privacy policies that they must follow and will receive guidance from their agencies. This User Policy only applies to HMIS policies and procedures.

Users will only view, obtain, disclose, and use the HMIS database information when necessary to perform their job, which may include coordinating services for a client.

Users need to complete a client Release of Information (ROI) with each client before entering client information into the Austin / Travis County HMIS system. Users shall ensure that prior to obtaining a client's permission on the ROI, they fully review the ROI with the client in a manner that ensures that the client fully understands the information (e.g. securing a translator, if necessary). All information that a client provides will be entered into the Austin / Travis County HMIS system and shared with any Partner Agencies; however, it is the client's decision about the information they provide. Users will not deny services to a client because they refuse to answer a question, unless that information is necessary for determining their eligibility for services. Users will provide clients with a copy of the ROI upon request.

Users shall only put treatment records about Mental Health, HIV/AIDS, or Drug, Alcohol, or Substance Abuse Treatment into HMIS when the client provides verbal or written permission on the ROI to put treatment records in HMIS.

Users shall only share client information outside of HMIS, including discussing client information outside of HMIS or sharing client information with outside agencies for coordinating services, when the client provides verbal or written permission to do so on the ROI. The client will select the specific outside agencies that they permit data sharing for the purposes of coordinating services. User shall only share client information with agencies outside of HMIS for the purposes of research and reporting after getting approval from ECHO and after ECHO has completed a formal data sharing agreement with the outside agency receiving the data.

The Privacy Notice should be posted wherever staff are working with clients. Users shall make clients aware that the Privacy Notice and Privacy Policy Statement documents are available for their review. These documents outline the Austin / Travis County HMIS privacy policies. Users shall ensure that upon client request they fully review the Privacy Policy Statement with the client in a manner that the client fully understands the information. Users will provide clients with a copy of the Privacy Notice and Privacy Policy Statement upon request.

Client Confidentiality

Clients who come to HMIS participating agencies for assistance confide things about themselves or their families, which is often of a very personal and private nature. Participating agencies and Users are obligated to protect client confidentiality by not disclosing information to third parties without a client's permission. If a client provides verbal or written permission on the ROI that their personal information can be shared outside of the HMIS system, then Users may discuss that information directly with other HMIS Agencies or release that information to the specific Outside Agencies permitted by the client on the ROI, only when that sharing of information is necessary for the User to perform their job.

Release of Information (ROI)

Users are sensitive to the fact that clients lose some of their privacy when they answer HMIS questions such as questions about income, benefits, and experiences with homelessness. Clients must be informed that all information they provide will be shared with other HMIS Agencies and receive a thorough explanation of the reasons why information is shared. Clients should always be made aware that they have the right to refuse to answer any question at any time. Users have the responsibility of explaining the benefits of sharing information for clients to make informed information sharing decisions. Users can use language such as, "*The Austin / Travis County Continuum of Care works together to help individuals and their families resolve current or imminent homelessness and are dedicated to assisting people in obtaining and maintain permanent, safe, stable housing. Sharing your information may help you get services more quickly and easily, and it may also help multiple HMIS Agencies better coordinate services to meet your housing goals.*"

The Austin / Travis County Continuum of Care adheres to the federal guidelines of the U.S. Department of Housing and Urban Development (HUD) Homeless Management Information Systems (HMIS) data and technical standards, and the Health Insurance Privacy and Portability Act (HIPAA) for any agencies or data to which it applies. All information and services are strictly confidential. This means that:

- Information entered into the HMIS regarding clients, potential clients, or telephone contacts should only be viewed or obtained by users when necessary to perform their job, which may include coordinating services for a client.
- HMIS information cannot be disclosed to any source outside the HMIS system without the client's permission on the ROI. This includes discussing information from HMIS with other HMIS Agencies or releasing HMIS information to outside agencies, including utility companies, landlords, for making referrals, and emergency contacts.
- Users must take care to explain the details of how HMIS information may be shared, with whom it may be shared, and why it may be shared, both within and outside of the HMIS system.
- Within the User's agency, specific cases are not discussed with persons other than staff members that need to know the information to perform their job. This includes:
    - Conversation among staff members in the presence of non-agency staff or volunteers.
    - HMIS printed records are never made available to persons other than staff members who need that information to perform their job.
    - Only authorized agency users can view data contained with the HMIS system.

Users may hear the phrase "circle of confidence" in reference to sharing HMIS information. The circle of confidence in which HMIS information about a client may be shared includes supervisors and colleagues employed by the same agency where the client is receiving services but only when discussion of a client's case is appropriate. Only with a client-signed ROI consenting to sharing their HMIS information outside of HMIS may their information be shared outside of HMIS. Additionally, the client will select the outside agencies that they agree to share their information with.

If the User's agency is a HIPAA covered entity, the User will refer to their agency's policies and procedures regarding confidentiality as other restrictions may apply.

Law Enforcement

If a police officer comes to the User's agency requesting HMIS information about a client, the User will follow their agency's policies and procedures, which also include an appropriate response such as, "*We cannot tell you whether or not Mr. X is a client here, but if we do have a client by that name, we will encourage him to get in touch with you to discuss the matter.*"

If the officer comes back with a warrant, then it would be appropriate to breach confidentiality; in accordance with HMIS guidelines. However, the User will always contact their supervisor who will contact ECHO on issues such as these. Refer to the HMIS Privacy Policy Statement for detailed information on when HMIS information should be disclosed.

Emergencies

Confidentiality must be breached in certain emergencies, such as if the client is a danger to themselves or others, or if there is a situation where the User needs to report abuse or neglect of children or of the elderly or individuals with disabilities. Texas law instructs for disclosure to medical or law enforcement personnel where the professional determines that there is probability of imminent physical injury by the client to themselves or others. In any situation where the client makes a threat, ECHO recommends the User seek consultation from their supervisor.

Whenever the requirements of confidentiality are unclear, let the client do the informing. The User should use sound judgement: Agencies are legally responsible for the protection of client confidentiality. If the User has doubt whether to breach confidentiality in a specific circumstance, the User will contact their supervisor or ECHO. See the HMIS Privacy Policy Statement for detailed information regarding client confidentiality.

Electronic Files

ECHO requires that all original signed ROIs be uploaded to HMIS. Once uploaded, neither ECHO nor HUD require the agency to maintain the original paper document. In May of 2011, HUD released guidance on the use of HMIS as electronic documentation, which stated, "HUD does not require the maintenance of documentation in both paper and HMIS electronic record. Agencies must maintain all supporting documentation not entered or uploaded into the HMIS database to ensure that HMIS records meet HUD standards for completeness and sufficiency."

Prior to destroying and disposing the paper ROI document, each HMIS Agency must confirm that their agency and/or funders' recordkeeping policies do not require the original signed paper ROI document to be maintained.

Paper Files

All client information is confidential and must remain on the premises. Per HMIS policy, staff must secure printed copies of HMIS data. File cabinets containing HMIS data must be in a secure location and locked at the end of each day. Users must not keep any client files in unsecured locations, such as on their desks unattended or in unlocked drawers at night.

Paper files may include but are not limited to:

- HMIS Assessment Forms
- Signed client Release of Information
- HMIS reports containing client identifying information

The HMIS Policies and Procedures Manual includes more detailed information regarding storing paper files.

User Responsibility

Prior to receiving a HMIS username and password to allow a User to access to the HMIS system, the User must initial each item below to indicate training has been received and that the user understands and accepts the stated security policies, user policies, and code of ethics. Failure to uphold the confidentiality standards set forth is grounds for immediate termination from the HMIS system.

INITIAL EACH ITEM:

	My HMIS Username and Password are for my use only and must not be shared with anyone. I will take all reasonable means to keep my Password secure.
	A computer that has ServicePoint open and running will never be left unattended. If I am logged into ServicePoint and must leave the work area where the computer is located, I will log-off before leaving the work area.
	I will only view, obtain, disclose, or use the HMIS information that is necessary to perform my job.
	I understand data should be entered into the HMIS as close to real time as possible, but no more than 5 business days after the data is collected.
	I will not falsely record any information in HMIS. I will only enter what is accurate to the best of my knowledge and as the client reports.
	I understand that I have primary responsibility for information entered by me. Information entered must be truthful, accurate and complete to the best of my knowledge.
	I understand I am responsible for fully reviewing the ROI with the client in a manner that ensures that the client fully understands the information.
	I understand that the only individuals who can view information in ServicePoint are authorized users who need the information for legitimate business purposes of this Agency and the clients to whom the information pertains.
	I understand that it is the client's decision about the information they provide to be entered into HMIS. I will not deny services to a client because they refused to answer a question, unless that information is necessary for determining their eligibility for services.
	I understand that before any Client information is entered into HMIS, the client must provide verbal or written permission on the ROI; and that separate ROIs must be completed for each adult in a household. (Adults cannot sign to release information for other adults, unless they have documented, legal authorization to do so).
	I understand that if my agency is held to additional privacy restrictions by state or Federal law (such as HIPAA, VAWA, or Texas Substance Abuse Records regulations), it is my professional responsibility to ensure all appropriate additional consents are in place BEFORE I enter client information into the HMIS system.
	I understand that l will only put treatment records about Mental Health, HIV/AIDS, or Drug, Alcohol, or Substance Abuse Treatment into HMIS when the client provides verbal or written permission on the ROI to put treatment records into HMIS.
	I understand that I will only share client information outside of HMIS, including discussing client information outside of HMIS or sharing client information with outside agencies for coordinating services, when the client provides verbal or written permission to do so on the ROI.
	I understand that I must allow clients to update their information in HMIS or sharing preferences at the client's request.
	I understand that the original signed copy of a client’s ROI must be uploaded to HMIS and the client’s sharing authorization will last for seven (7) years. Once uploaded, neither ECHO nor HUD require the agency to maintain the original signed paper ROI document, unless my agency or funders’ recordkeeping policies require the original signed paper ROI document to be maintained.

	All paper copies of personally identifiable (client-level) information printed from ServicePoint must be kept in a secure file and destroyed when no longer needed.
	I will not enter “Client Doesn’t Know” or “Client Refused” when higher quality data are available.
	I understand that each Agency and User participating in the HMIS is fully legally responsible and accountable for the protection of client confidentiality.
	I understand that the HMIS Privacy Notice must be posted at all locations where the information is collected. I understand that I must make clients aware that there is a Privacy Policy Statement that clients can review and that I am responsible for reviewing the Privacy Policy Statement upon client request. I understand that clients must be given a copy of the Privacy Notice, Privacy Policy Statement, or client ROI upon client request.
	I understand that upon client request, I must allow a client to inspect and obtain a copy of the client's own information within the ServicePoint HMIS database.
	I will not use the database for any violation of any law, to defraud any entity or conduct any illegal activity.
	If I notice or suspect a security breach, I must immediately notify the Executive Director of the Agency and the HMIS Director, Katy Manganella at (512) 481-2848 or katymanganella@austinecho.org

User Signature Date

User Work Phone User E-mail

Trainer’s signature Date

Appendix 4

Austin / Travis County Homeless Management Information System
Agency Administrator and Data Security Officer Authorization Form

Agency Name	
Address	
City	
State	
Zip	
Phone	
Agency Administrator Name and Title	

Authorization Agreement

I, _____, Executive Director or authorized individual of the above-named agency authorize the above-named employee as the ServicePoint Agency Administrator and HMIS Data Security Officer for this agency.

I understand that the above-named person will have top-level access to this agency's information in HMIS. I understand that HMIS Agency Administrators will have access to the following:

- Access to update client records including saving data, adding, and editing.
- Run agency reports on HMIS data.
- Edit this agency's information and can add, edit, and delete HMIS users for this agency.
- The Agency Administrator may not delete a client from HMIS. The Agency Administrator will contact ECHO HMIS if a client needs to be removed entirely from the database.

This individual will be responsible for:

- Completing HMIS Agency Administrator Training with ECHO HMIS.
- Ensuring all licensed HMIS users at this agency complete training prior to accessing the database and ensuring all HMIS users at this agency complete the annual Ethics Training.
- Maintaining workflow provided by HMIS for upholding the HMIS Data and Technical Standards.
- Attending HMIS Workgroup Meetings on behalf of this agency.
- Acting as the HMIS Data and Security Officer for this agency.

By this agreement, I authorize ECHO HMIS to give this employee the HMIS Access Level of Agency Administrator.

_____ _____

Signature Date

Appendix 5

Austin / Travis County Homeless Management Information System
Data Quality Assurance Plan

Purpose: Data quality refers to the timeliness, completeness, and accuracy of information collected and reported in the Homeless Management Information System (HMIS). The U.S. Department of Housing and Urban Development (HUD) set parameters around data quality in the HMIS Requirements Proposed Rule published in December 2011. This Data Quality Assurance Plan will be updated once the HMIS Final Rule is published. The purpose of this Plan is to establish **minimum** standards for quality assurance and client tracking that uphold the interim standards set by HUD.

The Austin/Travis County HMIS Quality Assurance Plan outlines policies and procedures that all participating agencies must implement to ensure the data integrity of agencies/programs.

Policy: Participating agencies will provide the following levels of data accuracy and timeliness for each program within HMIS:

- All data entered in HMIS will be as accurate and complete as possible.
- All Date of Birth entries will be entered as provided by the client or best estimate of the birth year with the month/day of 01/01 of the approximate year if the client does not provide an exact answer. (See HMIS Data Standards Manual for more information)
- The total number of Blank or Null entries for the Universal Data Elements (UDEs) and their associated "Data Quality" fields will not exceed 3% per month.
    - Null Values are data fields where the answer is missing or not entered.
- The total number of entries that are "Refused", "Refused (HUD)", "Don't Know" and "Don't Know (HUD)" will not exceed 5% per month.
    - Don't Know/Don't Know (HUD)/Don't Have is used when the client provides that answer for a question.
    - Refused/Refused (HUD) is used when the client provides that answer for a question.
- Data entry must be completed in HMIS by the 5th business day after the date of applicable client interaction or program entry/exit.

Procedure: The participating Agency Administrator will perform regular data integrity checks on the participating agency's programs within HMIS. Any patterns of error at a participating agency must be corrected. The participating agency will provide a copy of the report(s) to the HMIS Director by the tenth (10th) day of the following month, or the following business day if the 10th falls on a weekend or holiday. The ECHO HMIS personnel will monitor all participating agencies on their data entry techniques and for compliance.

1. Run the custom report "ECHO HMIS Data Completeness Report Card (EE) – v#" for all programs within HMIS for the participating agency.

2. Create QA Findings sheet for non-compliant agencies/programs and submit to ECHO HMIS and timelines for correction.

3. Rerun reports for errant agencies/programs. Follow up with the ECHO HMIS Director or HMIS Administrator if necessary.

4. ECHO HMIS will provide the participating agency Executive Director with an overall report card.

Participating Agency Responsibilities:

Participating agencies agree to:

1. Assure the accuracy of information entered into HMIS regardless of who entered the data that is not or is no longer accurate. Any updates in information, error or inaccuracy that comes to the attention of the participating agency will be corrected by such agency.
2. Perform routine Quality Assurance procedures to monitor data quality and promptly correct inaccuracies.

- **Data Tracking of Client Services:**
  1. The participating agency must track entries and exits into HMIS programs in HMIS. This includes entry, exit, and update assessment data for clients served and recording exit outcome information in HMIS.
  2. The participating agency must implement client record keeping procedure(s).
  3. Residential projects will maintain up-to-date information in HMIS about who is residing in the program.
- **Reporting Submission Deadlines:**
  1. Intake data should be entered into the HMIS **within five (5) business days of the completion of the intake process.**
  2. Shelters only: Clients who stayed in shelter during the previous 24-hour period shall be entered into HMIS daily **by 9:00am**.
  3. Complete and accurate data must be entered into HMIS by the 5th business day following the client interaction or program entry/exit.
- **Data Accuracy:**
  1. All clients must have unique ID numbers, which are generated by the HMIS upon record creation.
  2. Missing/Null data in HMIS must be **less than 3% per month in total for required fields**.
  3. "Refused", "Refused (HUD)", "Don't Know" or "Don't Know (HUD)" data in HMIS must be **less than 5% per month in total for required fields.**
     4. No data in HMIS can be incompatible with a program. For example, a family cannot be entered at a single men's shelter.
     5. Data in HMIS must accurately reflect client data recorded in the agency's client file and known information about the client and services provided to the client. For example, 'Exit Date' on the paperwork should be the date the client physically exited the program.
  6. Annual Assessments in HMIS are required for all clients who are active in a program for a year or more.
- **Data Consistency**
  1. Participating agencies will use consistent language to ensure a common definition of data.
  2. Measure consistency by making random interviews with users and ask how questions are worded with a goal of 90% consistency.
  3. Use common forms that accurately reflect HMIS for your program.
  4. Attend training on a regular basis, internally within the participating agency and externally through ECHO HMIS and others.
     a. ECHO HMIS provides the required annual Ethics Training.
     b. ECHO HMIS also provides additional training that covers using ServicePoint, Agency Administration, reporting and job-functional. This is not inclusive of all training that may be provided.

c. Each participating agency may provide program-specific training internally as needed.

d. ServicePoint users and Agency Administrators may have their HMIS access disabled until any required training is completed.

- **Data Quality Assurance**

1. Participating agencies shall have a Data Quality Assurance Plan that is Program-specific to assure quality data collection, entry, and reporting. A copy of the plan shall be provided to ECHO HMIS upon request.

The suggested schedule for Participating Agency Administrators to ensure high HMIS data quality:

Task	**Frequency**
Run the Data Completeness Report for each program and ensure corrections to data as necessary.	Monthly
Submit the Data Completeness Report for each program to ECHO HMIS.	Monthly - Required
Review the Data Completeness Report for each program and verify that missing data for required data elements does not exceed 3%.	Monthly
Validate that any paper files for the program match the HMIS data to ensure data accuracy.	Monthly
If in an Emergency Shelter, check bed list to verify accuracy in HMIS.	Weekly

Appendix 6

Austin / Travis County Homeless Management Information System
License and Support

End User Licenses

Each user must have a license to access the HMIS software, ServicePoint. The charge per license is $600 annually with the contract year of March 1 – February 28/29 each year. The following services and support are included with each license.

- The user license provides the named user access to ServicePoint after the required training has been completed.
- A user license for the ServicePoint Training Site. All training must be done within the Training Site and not the live ServicePoint site.
- PKI Security Certificate installation and management.
- All required HMIS user trainings will be provided by ECHO:
    - All new users are required to complete New User Training which includes privacy and ethics compliance training and HMIS application and workflow training.
    - For current users, an annual Ethics Refresher Training will be provided by ECHO for the user to maintain their HMIS license.
    - HMIS Agency Administrators are provided HMIS Agency Administration Training.
- Additional training will be offered throughout the year as changes occur or learning areas are identified.
- User support and technical assistance by ECHO.
- Creation of and assistance in defining program assessments and reporting requirements to meet grant and funder requirements.
- Technical assistance in and potential creation of custom reports. Complexity and required time constraints may require technical assistance from Mediware, the HMIS vendor, and additional charges would apply.
- Guidance and direction on HMIS and HUD-related requirements for participating agencies, Agency Administrators, and Agency Security Officers.
- ECHO will handle all vendor management with Mediware.
- Dedicated administration of HMIS to protect the privacy and confidentiality of data stored in ServicePoint.

Reporting Licenses

Users that need to generate advanced reports will need a Reporting License. Each participating agency is required to have **at least** one reporting license. There are two types of reporting licenses:

1. Ad-hoc License: $160/year, provides the ability to create custom reports and run standard and existing customized reports.
2. Viewer License: $90/year, provides the ability to run standard and existing customized reports.

Appendix 7

Austin / Travis County Homeless Management Information System
Privacy and Security Plan

Purpose:
Establish minimum privacy and security standards for the collection and maintenance of HMIS records for every client receiving services by participating agencies.

The Austin / Travis County HMIS Privacy and Security Plan outlines policies and procedures that all participating agencies must implement to ensure the privacy and security of client data input by agencies.

Policy:
Participating agencies will provide the following levels of privacy and security protection for each program within HMIS:

- Unique user name and password for each user
- Secure location for equipment used to access HMIS
- Locking screen savers and user profiles on computer equipment
- Virus protection with auto-update enabled
- Individual or network firewall
- Restrictions on access to HMIS via forums
- Compliance with the HMIS Policy and Procedures Manual
- Protection of all stored HMIS data

Procedure:
The participating Agency Administrator will perform quarterly privacy and security checks on the participating agency's programs within HMIS. Any area of non-compliance at a participating agency will be corrected immediately. The participating agency will provide the Privacy and Security Quarterly Compliance Assessment to ECHO HMIS upon request. The ECHO HMIS personnel can monitor all participating agencies on compliance with HMIS privacy and security standards. The assessment form is found in Appendix 8 of the HMIS Policies and Procedures Manual.

Participating Agency Responsibilities:

1. Assure the accuracy of information provided in the Privacy and Security Compliance Assessment. Any areas of non-compliance that comes to the attention of the participating agency will be corrected by the agency immediately.
2. Maintain a file of the Privacy and Security Compliance Assessment along with any supporting documentation. ECHO HMIS may ask for these records at any time.
3. Provide the HMIS Director with a copy of the Privacy and Security Compliance Assessment upon request.

Appendix 8

Austin / Travis County Homeless Management Information System
Privacy and Security Assessment Form

Agency Name	
Assessment Date Range	

Compliance Area	Yes	No
All users that access HMIS have a unique name and password.		
Equipment is in a secure location.		
Devices that access HMIS have locking screen savers and user profiles.		
Devices that access HMIS have an individual or network firewall.		
Access to HMIS is restricted via public forums.		
The agency complies with the HMIS Policies and Procedures Manual.		
The agency has the appropriate protections in place for all stored HMIS data.		

If applicable, the compliance area(s) that are non-compliant will be corrected by the following steps:

I certify that the information provided is true and accurate to the best of my knowledge.

Agency Administrator Name Signature Date

Appendix 9

Austin / Travis County Homeless Management Information System
Data Sharing Policy and Release of Information (ROI)

Agency Completing Form: _____

This agency collects information about people who ask about our homeless services. When we meet with you, we will ask you for information about you and your family. We will put the information you give us into a computer program called Mediware ServicePoint (or "HMIS").

Austin / Travis County HMIS data is all stored in one computer system. Your information will be shared with all agencies that use our system (all "HMIS Agencies") to help you get services more quickly and easily. A list of all current HMIS Agencies is on the next page of this form, and you can ask for a new copy at any time.

The Personal Information we share may include:

- Personal Identifying Information (such as name, social security number, and date of birth)
- Who is in your household
- Job history
- Military history
- Living situation and housing history
- Educational background
- Demographic information (such as race, gender, and ethnicity)
- Your income and income sources
- Services you request or receive
- If you are experiencing homelessness or not
- Reasons for seeking services
- Self-reported health needs

You can refuse to answer **any** question at **any** time, including questions about the things listed above. You will **never** be denied help because you did not answer a question, unless we need to know that answer to know if you are eligible for a service.

We will not store or share treatment records about Mental Health, HIV/AIDS, or Drug, Alcohol, or Substance Abuse Treatment unless you give us specific permission.

We may also share some of your information from HMIS with agencies that do not use our HMIS system ("Outside Agencies") for different summary reports about homelessness. Personal Information that could be used to tell who you are will only be put in those reports if we have your written permission, or if the law lets us or requires us to share that information without your permission.

_____ **Please initial here to show that you have read and understand the rules above.**

Consent for Release of Personal Information
In addition to the information sharing above, you can also choose:

- To let HMIS Agencies share and discuss your Personal Information outside of the computer system to help give you services;
- To let HMIS Agencies share your Personal Identifying Information with Outside Agencies for research, reporting, and coordinating services; and
- To let HMIS Agencies put any treatment records about Mental Health, HIV/AIDS, or Drug, Alcohol, or Substance Abuse Treatment into our computer system as part of your Personal Information.

Please think about the information below before making your decisions:

- Personal Information that can be used to tell who you are (Personal Identifying Information) will only be shared with Outside Agencies with your permission, or when the law lets us share that information without your permission.
- If you let us put any treatment records related to Mental Health, HIV/AIDS, or Drug, Alcohol, or Substance Abuse Treatment into our computer system, we will share that information just like the rest of your Personal Information.
- The current list of HMIS Agencies is below. Any agency not on that list is considered an Outside Agency. Other agencies may join this list in the future and share your information just like the current HMIS Agencies. You may ask for an updated list of the HMIS Agencies from **any** HMIS Agency at any time.
- Some of your Personal Information may be protected by additional state and federal privacy laws. Agencies that must follow these laws may need additional permission to collect or share some of your information.
- Once we share your information with an Outside Agency, that agency can sometimes share it with other Outside Agencies, if the law says they can.
- This consent is voluntary. You will **not** be denied services if you decline to sign this consent form.

Current Austin / Travis County HMIS Agencies:

- A New Entry
- AIDS Services of Austin
- Any Baby Can
- Austin Recovery
- Austin Voices for Education and Youth
- Caritas of Austin
- Casa Marianella
- Catholic Charities of Central Texas
- City of Austin – CDU, DACC, EMS
- CommUnity Care
- Ending Community Homelessness Coalition (ECHO)
- Family Eldercare
- Foundation Communities
- Foundation for the Homeless
- Front Steps
- Seton Good Health Solutions Center
- Goodwill Industries of Central Texas
- Green Doors
- Housing Authority – City (HACA)
- Housing Authority of Travis County (HATC)
- Integral Care
- LifeWorks
- LINC Austin
- Meals on Wheels and More
- Mobile Loaves and Fishes
- SAFE Alliance
- Saint Louise House
- Sunrise Homeless Navigation Center
- The Salvation Army
- Travis County – Health & Human Services & Veteran Services
- Travis County – Mental Health Public Defenders
- Trinity Center
- U.S. Department of Veteran Affairs

Optional Agencies Section

Please choose one:

_____ **Yes**, all Austin/Travis County HMIS Agencies may share and discuss Personal Information about me and my family outside of the computer system to help give us services. They may also share that information with Outside Agencies for research, reporting, and coordinating services.

Permission to share your information will last for seven years from the date you sign this form. You can cancel this permission at any time by sending a written letter to the agency where you filled out this form. It may take up to three business days to process the cancellation letter.

_____ **No**, I do not want HMIS Agencies to share and discuss my Personal Information outside of the computer system. I also do not want information that can be used to tell who I am to be part of any outside reports or research. HMIS Agencies may only share information in the computer system for questions I choose to answer.

If you chose **NO** above, you can still choose to let HMIS Agencies share and discuss your Personal Information **with specific Outside Agencies or individuals** outside of the computer system to coordinate services. If you want to do that, please initial your choices below.

_____ Contact Person: _____

_____Austin Police Department
_____Capital of Texas Workforce
_____Community Care Collaborative
_____Dell Medical Center
_____Dept. of Assistive & Rehab Services
_____Integrated Care Collaborative
_____Managed Care Organizations
_____Seton/Brackenridge Hospitals
_____Social Security Administration
_____St. David's Hospital
_____TX RioGrande Legal Aid
_____Other
_____Other

Optional Treatment Records Section

Please initial below if you would like to put treatment records about Mental Health, HIV/AIDS, or Drug, Alcohol, or Substance Abuse Treatment in our computer system as part of your Personal Information. We will share this sensitive health information for the record types you initial below:

_____Mental Health Treatment Records

_____HIV/AIDS Test Results and/or Treatment Records

_____Drug, Alcohol, or Substance Abuse Treatment Records

Client Name: _____

Dependents Name(s): _____

Client or Representative Signature: _____ Date: _____

Witness Signature: _____ Date: _____

FOR ORGANIZATIONAL USE ONLY (Initial all that apply):

( ) The client received a telephonic explanation of this form. Staff obtained telephonic acknowledgement of HMIS Data Sharing Policy and documented that consent with the staff signature on this form.
( ) The client wishes to remain anonymous in HMIS.
( ) An authorized representative completed this consent for the client. A description of their right to do so is attached.
( ) Other: _____

Appendix 10

Austin / Travis County Homeless Management Information System
Privacy Policy Statement

This agency collects information about people who ask about our homeless services and puts the information you give us into a computer program called Mediware Information Systems ServicePoint (or "Austin/Travis County HMIS"). Austin/Travis County HMIS data are all stored in one computer system maintained by the Ending Community Homelessness Coalition (or "ECHO"). This Privacy Policy Statement describes the practices connected with the Austin/Travis County HMIS computer program. A link to this Privacy Policy can be found on the HMIS section of the ECHO website. A copy of this Privacy Policy Statement, the Privacy Notice and the Data Sharing Policy and Release of Information are available to clients upon request.

Scope
The Privacy Policy only applies to the information entered in to the Austin / Travis County HMIS computer system and does not apply to any other website or computer system. We only collect information that we think is appropriate. The collection and use of all personal information is guided by strict confidentiality standards as outlines in this Privacy Policy Statement.

This document is not a legal contract. We are required to provide and follow the practices described in this Privacy Policy. This Privacy Policy takes effect immediately and will remain in effect until we replace it. The Privacy Policy can be amended. Any changes may affect the use of information collected before the policy change.

Purpose of Data Collection
When agencies that use the Austin / Travis County HMIS computer system meet with you, they may ask you for information about you and your family. We may be required to collect some personal information by law or by organizations that give us money to operate this program. Additional personal information that we collect is important to run our programs, to improve the services for people experiencing homelessness, and to better understand the needs of people we serve.

YOU HAVE THE RIGHT TO REFUSE TO ANSWER **ANY** QUESTION AT **ANY** TIME AND YOU WILL NOT BE DENIED HELP, UNLESS WE NEED THAT INFORMATION TO KNOW IF YOU ARE ELIGIBLE FOR A SERVICE.

What personal information is collected about you?
- Personal identifying information (such as name, social security number, and date of birth)
- Demographic information (such as race, ethnicity, and gender)
- Who is in your household
- Your income and income sources
- Job history
- Services you request or receive
- Military history
- Housing status and history
- Current living situation
- Reasons for seeking services
- Self-reported health needs

What happens to your information?
- When you request services from agencies that use the Austin / Travis County HMIS computer system, the agency will review the client Release of Information (ROI) that describes the data sharing rules within and outside of the computer system.
- After you acknowledge that you understand the data sharing rules, your information will be entered into the Austin / Travis County HMIS computer system, which is operated over the internet. The

Austin / Travis County HMIS uses many security protections, as listed in the Security and Confidentiality section of this Privacy Policy, to ensure confidentiality.

- Your current and historical information will be shared with all agencies that use the Austin / Travis County HMIS system to help you get services more quickly and easily. We also share your information to help you get better services from our agencies. All current HMIS Agencies are listed on the client ROI document.
- If you provide verbal or written permission on the client ROI that you want to put treatment records about Mental Health, HIV / AIDS, or Drug, Alcohol, or Substance Abuse Treatment into our computer system as part of your personal information, that information will be entered into the Austin / Travis County HMIS system and will be shared with all agencies that use the system.
- If you provide verbal or written permission on the client ROI for the additional sharing of your data outside of HMIS, then you and your family's current and historical information in the Austin / Travis County HMIS system may be shared directly outside of the computer system or with outside agencies for research, reporting, and coordinating services.

Uses and Disclosures of your Personal Information

Once you acknowledge that you understand the Austin / Travis County HMIS data sharing rules, your current and historical data may be used or shared to:

- Provide and coordinate services to you and your family
- Carry out functions related to payment or reimbursement of services
- Carry out administrative functions, such as legal, audit, and management functions
- Provide different summary reports about homelessness as required by law or by the organizations that provide money for these programs
- Create deidentified reports for additional analysis
- Meet the requirements of the law
- Prevent a serious threat to health or safety
- Report abuse, neglect or domestic violence to a government authority authorized by law to receive these types of reports when required by law, or when the individual agrees to the disclosure, or when the disclosure is allowable by regulations and we feel it is necessary to prevent serious harm to the individual or other potential victims.
- Comply with law enforcement requests such as in response to a lawful court order, court-ordered warrant, subpoena or summons issued by a judicial officer, or a grand jury subpoena; a limited and specific inquiry approved by a supervisory official of the law that is necessary for a law enforcement investigation
- Learn about how well we are serving our clients and to find new ways to improve those services
- Understand the scope of need for our services in Austin / Travis County and to use that information when making decisions about ways to end homelessness

If you provide verbal or written permission on the client ROI for the additional sharing of your data outside of HMIS, then you and your family's current and historical information may be shared directly outside of the computer system or with outside agencies for the following reasons:

- To help you get services quickly and easily
- To help you get better services from our agencies and coordinate your services
- For research and reporting conducted by an individual or institution that has a formal relationship and a written data sharing agreement with ECHO that must:
    1. Establish rules and limitation for the processing and security of the information
    2. Provide for the return or proper disposal of the information after the research project is over
    3. Restrict additional use or disclosure of client personal information, except where required by law, and
    4. Require that the recipient of data formally agree to comply with all terms and conditions of the agreement

Security and Confidentiality Guidelines

- The Austin / Travis County HMIS operates over the internet. The site is encrypted with a security certificate that keeps the site secure and the information in it protected. Only agencies that use HMIS in Austin / Travis County can view and enter information into the Austin / Travis County HMIS system. Austin / Travis County HMIS users have a password-protected login to the system. Also, Austin / Travis County HMIS users receive training on the privacy and security standards outlines in this Privacy Policy Statement and must sign a confidentiality agreement where they agree to comply with this Privacy Statement.
- Agencies using the Austin / Travis County HMIS will uphold federal and state confidentiality regulations to protect client records and privacy. In addition, they will only release client records outside of the Austin / Travis County HMIS computer system with written consent by the client, unless otherwise provided for in the regulations.
- Agencies using the Austin / Travis County HMIS must abide by the HMIS Privacy Policy and Security Standards as outlined in the HMIS Data and Technical Standards. The Privacy Policy Statement was written in accordance with those standards.
- Agencies using the Austin / Travis County HMIS will abide specifically by the federal confidentiality rules regarding disclosure of alcohol and/or drug abuse records.
- Agencies using the Austin / Travis County HMIS will abide specifically by State of Texas, the City of Austin, or Travis County general laws providing guidance for release of client-level information including who has access to client records, for what purpose and audit trail specifications for maintaining a complete and accurate record of every access to and every use of any personal data by persons or organizations.

What are your rights under the Privacy Policy?

- You can refuse to answer **any** question at **any** time, including questions about the things listed on in this Policy. You will never be denied help because you did not answer a question, unless we need to know that answer to know if you are eligible for a service.
- Your permission to share your current and historical information will last for seven years from the date you sign the client ROI. You can cancel this permission at any time by sending a written letter to the agency where you filled out this form. It may take up to three business days to process this cancellation letter.
- You have the right to view and get a copy of your information that is entered into the Austin / Travis County HMIS system, except in circumstances such as in advance of legal proceedings, if there is information about another individual, if information was provided under a promise of confidentiality, if the sharing of the information would threaten the life or physical safety of an individual. You have the right to receive an explanation about any of your information that you do not understand.
- You have the right to request for a correction when your information in the Austin / Travis County HMIS system is incorrect or incomplete.
- You have the right to get a copy of this Privacy Policy Statement, the ROI, and the Privacy Notice if you request it.

Complaint Process:

If you have a complaint about the Austin / Travis County HMIS privacy and security policies and practices, please contact the ECHO HMIS Director.

ECHO – HMIS Director
300 E. Highland Mall Blvd., Suite 200
Austin, TX 78752

Or call the HMIS Director: (512) 481-2848