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 I 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