

**GEOCODE 489303 & 483288**

Continuum of Care Policies and Procedures

# HMIS/Community Database Policies & Procedures

Lubbock City & County Continuum of Care TX-625

## Version

Date	Version	Description
4/23/25	1.0	Initial release

<b>1. Introduction.....</b>	<b>3</b>
1.1 Purpose.....	3
1.2 Key Terms.....	4
1.3 Data Ownership.....	5
1.4 Voluntary Participation.....	6
1.5 ECHO HMIS/Database Documentation Amendment Process.....	6
<b>2. Stakeholder Responsibilities.....</b>	<b>7</b>
2.1 ECHO Board.....	7
2.2 CoC Board.....	7
2.2 Database Advisory Committee.....	7
2.3 ECHO.....	8
2.4 Participating Agency.....	10
2.5 Exempt Agency.....	11
<b>3. Operational Policies and Procedures.....</b>	<b>11</b>
3.1 Hardware, Software, and Network Requirements.....	12
3.2 System Access.....	12
3.3 User License Allocation Policies.....	13
3.3.1 Free License Allocation Policy.....	13
3.4 Data Collection Policies.....	16
3.5 Data Transfer.....	16
3.6 Training.....	17
3.7 Technical Assistance.....	18
<b>4. Security Policies.....</b>	<b>18</b>
4.1 Purpose.....	19
4.2 Policy.....	19
4.3 Applicability.....	20
4.4 Security Management and Compliance, Annual Review.....	20
4.5 Security Officers.....	20
4.6 ECHO Security Officer.....	20
4.7 Contributory Security Officer/Participating Agencies Security Officer.....	21
4.8 Disaster Recovery Plan.....	21
4.9 Security Awareness Training.....	21

4.9.1 Physical Safeguards.....	21
4.9.2 Technical Safeguards.....	22
Workstation Security.....	22
Establishing ECHO Database User IDs and Access Levels.....	22
Passwords.....	23
Rescinding User Access.....	23
4.10 Agency-Specific Data Security Policies and Procedures.....	24
<b>5. Privacy Policies.....</b>	<b>24</b>
5.1 Purpose.....	24
5.2 Privacy Notice.....	24
5.3 Purpose and Use Limitations.....	25
Authorized Uses of ECHO Database Data:.....	25
5.4 Participating Agency Data Sharing.....	25
5.4.1 Interagency Data Sharing / Client Consent.....	25
5.4.2 External Entity Data Sharing.....	26
5.4.3 Approval for research and community-level reporting.....	27
5.5. Data Requests.....	27
5.6 Client Consent.....	27
Procedures (Initial Consent).....	28
Procedures (Subsequent Consent).....	29
<b>Appendix I Privacy Notice (English &amp; Spanish).....</b>	<b>30</b>
<b>Appendix II Client Release of Information (ROI) (English &amp; Spanish).....</b>	<b>32</b>
<b>Appendix III Security Self Audit.....</b>	<b>36</b>
<b>Appendix IV Community Database Free License Application Form.....</b>	<b>38</b>

# 1. Introduction

## 1.1 Purpose

ECHO West Texas has established a localized community database known as the ECHO Community Database, which functions as the region’s Homeless Management Information System (HMIS). Required by the U.S. Department of Housing and Urban Development (HUD), HMIS participation is mandatory for recipients and sub-recipients of applicable federal grants. This system is essential for coordinating services, evaluating performance, ensuring accountability in the use of public funds, and informing public policy. It serves as the foundation for all planning to prevent, reduce, and eliminate homelessness.

The HMIS Lead in the TX-625 Lubbock County & City Continuum of Care (CoC) is ECHO West Texas (ECHO). ECHO is responsible for administering the local HMIS and must develop written policies and procedures for all agencies participating in the local HMIS/ECHO Database within the CoC's area of responsibility. ECHO is also responsible for execution of participatory Memorandums of Understanding (MOUs) with each agency and system user and to monitor and enforce compliance by all participating agencies with the requirements set forth in the participation agreement. ECHO is responsible for maintaining the HMIS/Community Database Policies and Procedures manual and all related documents, training system users, and providing technical assistance.

The software vendor for the Lubbock County and City CoC is WellSky Community Services.

## 1.2 Key Terms

**Continuum of Care:** a community-based collaborative that oversees homeless system planning and coordination, including the HMIS implementation

**ECHO West Texas (ECHO):** the organization that administers and operates the HMIS/Community Database, AKA HMIS Lead Agency

**Participating Agency:** any agency that contributes data or uses the HMIS/ECHO Database

**Exempt Agency:** any agency that is explicitly exempt from entering data into the HMIS by federal regulations. This includes victim services providers.

**Client:** a person who receives services at an ECHO Database participating agency

**Personally Identifiable Information (PII):** Defined in OMB M-07-16 as "...information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."

**Homeless Information Management System (HMIS):** refers to the database this document references. This system collects client level information to better provide services and to discover service needs in the community

**Memorandum of Understanding (MOU):** agreement between agencies, database users, and the ECHO Database Lead Agency

**Contributory HMIS Organization (CHO):** any organization that contributes data to the ECHO Database by entering data directly into the ECHO Database

## 1.3 Data Ownership

### 1.3.1 Data Ownership Policies

1. ECHO and the Contributory HMIS Organization (CHO) maintain joint ownership of the data entered into ECHO Database by the CHO.
  - A CHO can only request data from the ECHO Database that was entered by their organization or into a project owned by their organization.
  - A CHO can elect to no longer enter data into ECHO Database and may receive a copy of previously entered data, however, the data cannot be removed from the system and can still be used by ECHO for reporting and research purposes
2. Universal Data Elements are universally owned and can be requested by anyone who has entered data on the client's profile.
3. For projects with joint ownership, a primary and secondary owner must be established.
  - The primary owner maintains ownership of all data entered in the project.
  - The secondary owner may request data entered by their organization.
4. ECHO maintains primary ownership of data entered into the ECHO Database, but CHOs may request data that their organization has entered. (refer to Section 3.5, data transfer for further details)

### 1.3.2 Database Termination Procedures

1. In the event that the ECHO Database ceases to exist, participating agencies will be notified and provided reasonable time to access and save data on persons served by the participating agency. Thereafter, the information collected in the ECHO Database will be purged or appropriately stored.
2. In the event that ECHO ceases to exist or is no longer the administrator of the ECHO Database, the CoC Board will select a new HMIS Lead and transfer the custodianship of the data within the ECHO Database to another organization for continuing administration.
3. In such an event, participating agencies will be informed in a timely manner.

### 1.3.3 Requesting Data

1. When requesting data, the organization must identify all data elements being requested. Organizations may request Universal Data Elements, Program Specific Data Elements, and custom data elements
2. If data that is not linked to a project enrollment is requested (i.e. case notes), the ECHO Database Team will provide data linked to the Organization of the requestor.

3. Data requests must follow data ownership policies. Any data requested beyond the scope of ownership is subject to approval through the appropriate CoC committee.
4. For data sharing—interagency and external entity data sharing—refer to Sections 5.4 & 5.5

## **1.4 Voluntary Participation**

The CoC Board strongly encourages agencies that are not required to participate in ECHO Database that serve persons who are homeless or at risk of homelessness to participate voluntarily.

More homeless service providers, as well as other service providers, enables potential for:

- More effective coordination of client services through case management and referral information sharing
- More accurate tracking of client returns to the homelessness prevention and assistance system
- More accurate counts of homeless persons and system resources, which could be used to understand the gaps in the service system
- Better information about community-wide needs, which can help guide advocacy efforts, policymaking, and funding allocations
- Better information about system outcomes, which can be used to guide service targeting and performance efforts

## **1.5 ECHO HMIS/Database Documentation Amendment Process**

### **1.5.1 Policies**

The CoC and Database Advisory Committee will guide the amendment of the ECHO Database policies and procedures and other related documentation

The Database Advisory Committee will review and recommend approval of the ECHO Database Policies and Procedures and Data Quality Plan to the CoC Board.

### **1.5.2 Procedures**

1. Proposed changes may originate from any participant in the ECHO database, including clients.
2. When proposed changes originate within a participating agency, they must be reviewed the Executive Director/Program Director (or equivalent) and submitted to the ECHO Database manager
3. The ECHO Database manager will maintain a list of proposed changes

4. The list of proposed changes will be discussed by the Database Advisory Committee at the next regularly scheduled meeting. At this meeting, the committee will determine if these changes require additional research and, if so, they will create a plan for completing the necessary research.
5. If changes do not require additional research, or once this research is complete, then the committee will vote on whether or not to propose these changes to the CoC Board.
6. Changes recommended by the Database Advisory Committee will be made by the ECHO Database Manager and sent to all participating agencies
7. The Executive Director/Program Director (or equivalent) from each of the participating agencies shall acknowledge receipt and acceptance of the revised ECHO Database Policies and Procedures (or other documents) within 10 working days of delivery of the amended document by notification in writing or email to the ECHO Database manager. The agency's Executive Director/Program Director (or equivalent) shall also ensure the circulation of compliance of the revised policies and procedures within their agency.
8. Training on changes to database documentation will be scheduled as needed.

## 2. Stakeholder Responsibilities

### 2.1 ECHO Board

1. Select and designate an HMIS software
2. Work with the CoC to ensure consistent agency participation across the area
3. Evaluate performance of Database software and ECHO

### 2.2 CoC Board

1. Select and designate an HMIS Lead for the CoC, among Eligible applicants
2. Work with the HMIS Lead to ensure consistent agency participation across the CoC
3. Evaluate performance of the HMIS software and ECHO
4. Approve governing database documents based on the recommendations of the Database Advisory Committee

### 2.2 Database Advisory Committee

1. Review and recommend for approval the ECHO Database policies and procedures
2. Review and recommend for approval the Data quality plan

3. Gather and incorporate user feedback into the ECHO Database policies and procedures
4. Provide feedback on ECHO Database documentation
5. Participate in efforts to promote ECHO Database operations, research and analysis

## **2.3 ECHO**

1. ECHO West Texas (ECHO) is responsible for the administration of the ECHO Database project under the auspices of the CoC Board, which authorizes ECHO as the HMIS Lead Agency
2. ECHO shall maintain a Database Administrator dedicated solely to those Database responsibilities set forth in this section. These are grouped by function, though job titles and descriptions may differ.
3. ECHO shall enable participating agencies and system users to receive professional technical assistance.

### **2.3.1 ECHO Database Manager**

1. Oversee Collection, analysis and presentation of ECHO Database data for reporting to federal, state, and local governments, and private entities
2. Oversee reporting process for HUD and HMIS grant application as needed
3. Oversee overall administration of ECHO Database software
4. Oversee ECHO Database department activities and staff as described in this section

### **2.3.2 ECHO System Administrator**

1. Leads team in maintaining system performance
2. Maintains security, maintenance, backups, and capacity of the ECHO Database database
3. Lead team in identifying data quality problems, developing remedies, suggesting and implementing corrective and/or preventative actions
4. Lead team in system troubleshooting and continuous improvement efforts
5. Establishes team standards and practices for monitoring timely and accurate completion of critical data elements and processes
6. Provides technical guidance in identifying and defining data elements stored in the system
7. Reviews data queries and reports for accuracy
8. Leads team in implementing required HUD Federal Reports and Data Standards requirements
9. Assists user organization in requirements gathering, process documentation, and other business analysis
10. Establishes and maintains documentation, change management, and testing and development procedures for customization and enhancements

11. Coordinates activities related to software updates and upgrades, including communication with ECHO Database manager and other organization staff, software testing and implementation scheduling

### **2.3.3 ECHO Database Security and Compliance Coordinator**

1. Complete site visits at participating agencies to monitor compliance with ECHO Database Policies and Procedures
2. Assist in developing the ECHO Database Security Plan
3. Document reports of suspected violations of client privacy or data security policies, participating agency responses, and ECHO responses
4. Coordinate with ECHO Database Manager regarding ECHO responses to suspected violations of client privacy and data security policies
5. Coordinate with participating agencies regarding agencies policy of disposal of electronic devices where clients' Protected Health Information (PHI) was stored
6. Serve as point of contact on HMIS Data Standards compliance, staying abreast of any changes
7. Maintain the ECHO Database Policies and Procedures document, making updates and revisions as needed
8. Ensure compliance with HUD HMIS Data and Technical Standards and ECHO ECHO Database policies and procedures

### **2.3.4 ECHO Database Training Coordinator**

1. Conduct training for all ECHO Database users, including but not limited to ECHO Database security awareness training, HMIS Fundamentals Training, Elements of Focus Training, Program Specific Training, Report Training, Chronic Homeless Definition Training, System Performance Measures Training, Point in Time Training
2. Responsible for providing and creating training materials, including training guides, tutorial videos, and other resources as requested
3. Provide technical guidance on ECHO Database implementation to participating agencies
4. Conduct Annual security training for system users.

### **2.3.5 ECHO Database System Administrator**

1. Oversee ECHO Database system performance
2. Work closely with HUD and Software vendors to ensure compliance
3. Maintain contact with ECHO Database software vendor to ensure optimal performance
4. Ensure the ECHO Database is secure
5. Identify problematic areas and conduct research to determine the best course of action to correct the data
6. Analyze and solve issues with current and planned systems as they relate to the management of client data
7. Analyze reports of data duplicates or other errors to provide ongoing appropriate interdepartmental communication and monthly or daily data reports

8. Provide technical assistance to users
9. Activate/disable user accounts
10. Assist with data monitoring within ECHO Database

#### **2.3.6 ECHO Database Data Quality Analyst**

1. Work with participating agencies to maintain accurate Housing Inventory Count within HMIS
2. Work with ECHO Database advisory Committee to devise and monitor quality benchmarks
3. Assist in defining specifications for updates to data elements in the ECHO Database
4. Assist participating agencies with performance evaluation activities
5. Complete data analysis projects
6. Fulfill external data requests as approved
7. Provide support to system users and their use of ECHO Database data

## **2.4 Participating Agency**

#### **2.4.1 Agency Executive Director/Program Director**

1. Sign the Contributory HMIS Organization (CHO) Agreement and submit it to the ECHO Database Security and Compliance Coordinator
2. Ensure agency compliance with terms and conditions of the CHO Agreement and ECHO Database Policies and Procedures
3. Ensure personnel with access to the ECHO Database comply with the terms and conditions of the Security Awareness Agreement
4. Designate one employee as the agency's Database Representative to service as the primary point-of-contact on Database operations at the agency
5. Designate one employee as the agency's Database Security officer and notify the ECHO Database Security and Compliance Coordinator of this assignment
6. Support ECHO's effort to resolve Database data quality and compliance issues

#### **2.4.2 Agency Database Representative**

1. Ensure compliance with ECHO Database data collection, data entry and reporting requirements as outlined in the ECHO Database policies and procedures
2. Serve as primary point-of-contact for communication between the agency and ECHO on ECHO Database operations
3. Provide support on resolution of any data quality and reporting issues
4. Identify agency personnel to access the system and receive ECHO Database training
5. Notify ECHO Database staff within 24 hours of relevant personnel changes to ensure system user accounts are deactivated

#### **2.4.3 Agency Database Security Officer**

1. Ensure compliance with the privacy and security standards as outlined in the ECHO Database policies and procedures
2. Send a copy of agency-specific data security policies and procedures to the ECHO Database Security and Compliance Coordinator
3. Send updated agency-specific data security policies and procedures to the ECHO Database security and compliance coordinator within 30 days of any changes
4. Ensure compliance with the agency specific security policies and procedures
5. Document and investigate suspected violations of client privacy or data security policies
6. Notify ECHO Database security and compliance coordinator within 24 hours of receiving reports of suspected violations of client privacy and data security policies
7. Notify ECHO Database security and compliance coordinator of the agency's response to suspected violations of client privacy and data security policies

#### **2.4.4 System End User**

1. Sign the End User Memorandum of Understanding (MOU)
2. Responsible for upholding MOU when operating within the ECHO Database
3. Complete ECHO Database training and meet objectives
4. Comply with all ECHO Database agreements, policies and procedures
5. Report suspected violations of client privacy and data security policies to the agency Database security officer
6. Provide feedback to ECHO

### **2.5 Exempt Agency**

1. An agency which—by reason of law, regulation, or funding—is barred from participation in a shared database
2. Utilize a database comparable to the HMIS
3. Develop database policies and procedures that comply with federal regulations
4. Submit policies and procedures to the ECHO Database security and compliance coordinator
5. Ensure compliance with agency-level policies and procedures

## **3. Operational Policies and Procedures**

## 3.1 Hardware, Software, and Network Requirements

The participating agency is responsible to meeting the minimum hardware, software, and network requirements to access the ECHO Database, and for providing the necessary maintenance for continued participation

The ECHO database is a web-based application that can be accessed from any desktop computer (PC or Mac). It may have limited functionality on mobile devices like smartphones; however, tablets and iPads should have full functionality. In order to access the ECHO database, the device must be connected to the internet and have one of the following browsers installed:

- Google Chrome 50.0 or above (Recommended)
- Firefox 40.0 or above
- Microsoft Edge

## 3.2 System Access

### 3.2.1 Policies

- The participating agency is responsible for identifying personnel for system training and access
- System users shall be assigned “roles” based on programmatic needs and considerations
- The participating agency will notify ECHO of any need to change “roles”
- The participating agency will notify ECHO of the need to deactivate system users within 24 hours of termination of their service with the agency. Advance notification is preferred especially in the case of agency-initiated termination

### 3.2.2 Procedures to Designate a New System User

1. The authorized contact will submit to the System Administrator the user’s first and last name, organization issued email address, role/title, and a description of system related job functions
2. The authorized contact must ensure the user as read and signed the End User MOU and is aware of the security/privacy policies and procedures of both the agency and CoC
3. The ECHO Database training coordinator will schedule applicable training(s) to occur within 5 business days of being notified of a new user’s need
4. Once the user has satisfied items in step 2, and the form has been submitted to the ECHO Database security and compliance coordinator, they will be granted access to the ECHO Database

### 3.2.3 Procedures to Change User Role

1. The authorized contact will request training from the ECHO Database training coordinator, and notify them of the need for a role change, specifying user’s first and last

name, organization issued email address, role/title, and a description of HMIS/Database related job functions

2. The training coordinator will either provide the required training and/or schedule the user for training. The user must complete the required training(s) prior to being assigned a new role

#### **3.2.4 Procedures to Deactivate a System User**

1. The authorized contact will submit a user deactivation request to the system administrator

2. The ECHO Database system administrator will deactivate the user's account

3. The participating agency can then reassign the deactivated user's license to a new user. Refer to section 3.2.2 for further guidance

### **3.3 User License Allocation Policies**

Refer to the most current version of the ECHO HMIS/Database pricing sheet for current pricing information and fee schedule.

Licenses are allocated to agencies but assigned to individual users. Should a licensed user, for whatever reason, no longer need access, the license can be assigned to another user in the agency for the remaining term of the license. Additional licenses can be requested and purchased at any time by the agency with a request to the system administrator at ECHO. Refer to section 3.2.2.

Participating agencies will be invoiced annually for user licenses. Invoices will be sent at least 30 days before the renewal date of user licenses. Should the invoice be unpaid 60 days after the invoice date, the current user licenses will be suspended until the invoice is paid.

#### **3.3.1 Free License Allocation Policy**

Housing providers receive one (1) free user license. Non-Housing organizations that have agreed to be Coordinated Entry Points will receive one (1) free user license. For organizations outside of these categories, free licenses are allocated according to this policy:

##### **3.3.1.1 Purpose**

The purpose of this policy is to define the criteria and process for allocating free licenses for the use of the Community Database. The policy ensures fair and equitable distribution while prioritizing organizations that align with the community's mission and values.

**Note:** Free licenses are awarded for a period of one (1) year. Any organization that receives free license(s) should ensure it is able to maintain that license in the event free licenses are unavailable when attempting to renew their free license(s). Organizations that are granted free licenses should be aware that these licenses are contingent upon the availability of grant funding. This funding may not be sufficient to cover costs for more than a single year. Therefore, any organization that benefits from a free license should proactively develop a sustainability plan to ensure they can maintain the license in the future. This is especially crucial in scenarios where grant funding for free licenses becomes unavailable at the time of renewal. Organizations need to be prepared to assume the financial responsibility of the license to avoid any disruption in service or access.

### 3.3.1.2 Eligibility Criteria

Organizations requesting a free license must meet the following criteria:

- a. **Non-Profit Status:** The organization must be a registered non-profit, charity, or community-based organization.
- b. **Mission Alignment:** The organization's mission should align with the goals of the Community Database, such as promoting social welfare, education, public health, or community development.
- c. **Financial Need:** Organizations must demonstrate financial constraints that prevent them from purchasing a license at full cost.
- d. **Community Benefit:** The organization should demonstrate how access to the database will directly benefit the community or marginalized groups.
- e. **Non-Commercial Use:** The organization must not use the database for commercial purposes, including selling or redistributing data for profit.
- f. **Data Privacy Compliance:** The organization must adhere to applicable data privacy and protection policies and regulations.

### 3.3.1.3 Application Process

Eligible organizations must submit a formal application (Appendix IV) including:

- a. A completed application form detailing the organization's mission, intended database use, and expected impact.
- b. Proof of non-profit status (e.g., tax-exempt certification or equivalent documentation).
- c. A statement of financial need outlining why a free license is required.

d. A letter of commitment ensuring adherence to data privacy and usage policies.

#### **3.3.1.4 Review and Approval**

Applications will be reviewed by the ECHO Team / Finance Committee based on the following criteria:

- a. The relevance and impact of the organization's work in relation to the community database.
- b. The extent to which the license will enable positive community outcomes.
- c. The organization's compliance with data protection and privacy policies.
- d. The availability of free licenses based on current allocations and budget constraints.
- e. Organization size, budget constraints, serving high priority need, or has emergency/temporary need for a license

The review process will be conducted quarterly, and successful applicants will be notified via email.

#### **3.3.1.5 License Terms and Conditions**

Organizations granted a free license must adhere to the following conditions:

- a. The license is valid for a period of one (1) year and subject to renewal upon review.
- c. The license is non-transferable and cannot be resold or sublicensed to another organization.
- d. Organizations receiving a free license must regularly update their service and organizational information to ensure accuracy and relevance.
- e. Organizations receiving a free license must, at minimum, utilize the Community Database to receive and resolve referrals within the timeframes designated in the various ECHO West Texas policies and procedures.
- f. Organizations receiving a free license, must adhere to all policies and procedures governing the Community Database.
- g. Non-compliance with the policy terms may result in license revocation.

#### **3.3.1.6 Policy Review and Updates**

This policy will be reviewed annually to ensure it remains relevant and aligns with the evolving needs of the community. Updates will be communicated to all stakeholders.

### **3.4 Data Collection Policies**

- The participating agency is responsible for understanding its own compliance and data collection requirements as may be defined by various grant programs and funders, and fulfilling any contractual obligations, including but not limited to compliance reports
- The participating agency is responsible for communicating these requirements to ECHO to ensure the system is properly configured to collect required data
- The participating agency is required to collect and enter information into the Database as defined in the federal HMIS Data Standards Manual
- The participating agency will be required to collect Local Data Elements as defined by the CoC and the Database Advisory Committee
- ECHO must provide training and technical assistance on Universal Data Elements and Project Descriptor Data Elements
- Refer to the participating agencies funding measures and scores for requirements that affect scoring and funding

### **3.5 Data Transfer**

#### **3.5.1 Policies**

- The participating agency is permitted to export data from ECHO Database to another system, once the agency has received written approval from ECHO to do so
- The participating agency is responsible for adhering to federal, state and local privacy laws within their databases, if it transfers any client data outside of the ECHO Database
- ECHO shall maintain a copy of all transferred data within the ECHO Database for reporting and research purposes.

#### **3.5.2 Procedures**

- The participating agency can request data transfer procedures from the ECHO by submitting a request through email.
- The CoC will coordinate data transfer between the participating agency and applicable software provider
- Should the data transfer incur a cost from the software provider, the participating agency is responsible for payment of these costs prior to the data transfer

## 3.6 Training

### 3.6.1 Policies

- All new users are required to complete ECHO Database system training and security awareness training before being allowed access to the system.
- All active users are required to complete annual training on security awareness
- All active users are required to participate in training on any updates to the system, policies and procedures, etc. as needed
- All users are required to sign the Security Awareness Agreement, acknowledging receipt of a copy of the privacy notice and pledging to comply with the privacy notice and additional terms and conditions for database access

### 3.6.2 Procedures

- ECHO Database training increases user's understanding, knowledge, and skills to effectively use the database
- Training is offered in a combination of online, digital, and live formats. Training may be requested for an entire department or individual one-on-one sessions

Optional and required trainings will be announced via email

### 3.6.3 Required Trainings and Training Sequence

The following user trainings are required before initial access is granted and at least annually thereafter:

1. Security and Privacy Training
  - a. Achieve score of at least 80% on the quiz to move forward
2. ECHO Database/HMIS End User Training, including data quality training & HMIS fundamentals
3. Coordinated Entry/Care Training, as appropriate

### 3.6.4 Required Trainings: Non-Attendance and Non-Compliance

When the user has selected a date for the applicable training(s) and does not attend or complete the training, the following steps are taken:

- 1st missed training: An initial notice is sent to the user; the agency manager and security officer are copied on the written communication. The manager must acknowledge receipt of email before user is rescheduled
- 2nd missed training: Within 24-hours of confirming the 2nd training was missed, another notice will be sent to the manager with the Agency Security Officer and user copies. The users' database access will be revoked within 48 hours until training can be scheduled and completed
- 3rd missed training: User access remains revoked. Access cannot be regained until a mandatory meeting is held with the ECHO Database trainer or manager, the user, and the user's manager/director.

## 3.7 Technical Assistance

### 3.7.1 Policies

- The participating agency may request ECHO Database technical assistance from ECHO
- Technical assistance is limited to operation and implementation of the ECHO Database for those authorized users as defined in these HMIS/Database Policies and Procedures

### 3.7.2 Procedure

- Requests for technical assistance can be submitted through email to the applicable ECHO Database staff member
- Technical support hours are Monday through Friday (excluding holidays) from 9am-4pm CST
- The requestor will provide issue details so that the issue can be recreated by the administrator in order to resolve the issue (screen shots, process taken to get to the error, etc.)
- The ECHO staff member will try to respond to all requests within 3 business days, but support load, holidays and other events may affect response time
- The ECHO staff member will submit a ticket with the HMIS vendor if progress on the issue is stalled
- If the support request is deemed by the system administrator to be an agency specific customization, resolution may be prioritized accordingly. ECHO reserves the right to charge on an hourly basis for these changes if/when the workload for such agency-specific customizations becomes burdensome
- ECHO staff may determine that the cause of the reported issue is outside the scope of control of the designated database
- ECHO staff will consolidate such requests from multiple partner agencies, if appropriate, and start to resolve issues in priority order according to their severity and impact
- If the ECHO staff is unable to resolve the issue, other software or system vendor(s) may be included in order to resolve the issue(s)
- In cases where issue resolution may be achieved by the Database User or other agency personnel, ECHO staff will provide instructions via email to the User and/or the agency contact

## 4. Security Policies

## 4.1 Purpose

- These security policies are directed to ensure the confidentiality, integrity, and availability of all ECHO Database information; protect against any reasonably anticipated threats or hazards to security; and ensure compliance by end users
- To promote the security of ECHO Database and the confidentiality of the data contained therein

## 4.2 Policy

For any participating agency that is required to be HIPAA compliant, the HIPAA rules for privacy and security supersede the requirements laid out in these policies and procedures. A HIPAA covered participating agency (HCPA) is responsible for defining security and privacy policies in its own policies and procedures. The HCPA must notify ECHO of its HIPAA status, provide its written security procedures, and make available/have posted its own HIPAA privacy notice. Refer to the 2004 HMIS Data and Technical Standards Final Notice for more information.

The security policies defined in this document are intended for non-HIPAA covered agencies participating in the ECHO Database

- An agency designates a Security Officer for monitoring security compliance. This must be updated at least annually or within 15 days of staff transition
- The Contributory HMIS Organization (CHO) Security Officer/Participating Agency Security Officer is responsible for preventing degradation of the ECHO Database resulting from viruses, intrusion, or other factors within the agency's control
- The participating agency security officer is responsible for preventing inadvertent release of confidential client-specific information through physical, electronic, or visual access to the workstation
- Each participating agency's security officer is responsible for ensuring it meets the Privacy and Security requirements detailed in the 2004 HUD HMIS Data and Technical Standards. Partner agencies will conduct a thorough review of internal policies and procedures regarding ECHO Database usage
- End users shall commit to abide by the governing principles of the ECHO Database and adhere to the terms and conditions outlined in the End User Memorandum of Understanding and the ECHO Database security awareness training(s)
- All users shall attend an annual security presentation
- All users and agencies will adhere to HUD 2004 data security standards
- Inform ECHO Database administrator within 24 hours of an employee leaving the agency for account deactivation
- Agencies and Users must consistently login to ECHO Database.

- After 30 days of a user/agency not logging in, their account will be suspended until a meeting between ECHO and the agency Director/Manager can be completed and a resolution made
- Participating agencies should conduct a security self audit (located in **Appendix III**) annually and report findings to ECHO.
- ECHO will conduct annual on site security audits using the security self audit (**Appendix III**) as a guide to such audits at participating agencies

### 4.3 Applicability

The participating agency and ECHO, including any authorized agents, must follow the security policies established in this section

### 4.4 Security Management and Compliance, Annual Review

- ECHO is responsible for managing the selection, development, implementation and maintenance of security policies to protect ECHO Database information
- ECHO must retain copies of all contract and agreements executed as part of the administration and management of the ECHO Database or otherwise required
- The security policies will be reviewed at least once annually to be approved by the CoC Board of Directors

### 4.5 Security Officers

The participating agency and ECHO must each designate an agency representative to serve as ECHO Database security Officer to be responsible for compliance with applicable security policies (see section 2, stakeholder responsibilities)

### 4.6 ECHO Security Officer

May be an ECHO Database system administrator or another employee, volunteer or contractor designated by ECHO who has been trained in, and has adequate skills in, assessing security compliance, current participating agency security measures for agency onboarding, reviews/maintains participating agency compliance certification checklists.

## 4.7 Contributory Security Officer/Participating Agencies Security Officer

- May be the agency's technical administrator or another employee within the agency, volunteer or contractor who has completed the privacy and security training and is adequately skilled to assess security compliance
- Conduct security audit for any workstation that will be used for ECHO Database data collection of entry
- Completes the compliance certification checklist and forwards the checklist to the ECHO security officer

## 4.8 Disaster Recovery Plan

- In the event of a disaster, recovery will be coordinated by the CoC and ECHO in collaboration with participating agencies and the applicable software vendors.
- The agency lead security officer should maintain ready access to the following information:
  - Contact information- phone number and email address of software vendor contacts
  - Agency responsibilities- a thorough understanding of the agency's role in facilitating recovery from a disaster
- All system administrators should be aware of, and trained to complete, any tasks or procedures for which they are responsible in the event of a disaster

## 4.9 Security Awareness Training

ECHO must ensure that all system users receive security training before being given access to the system(s) and at least annually thereafter. ECHO will maintain an attendance record(s) for all training events to assure compliance

### 4.9.1 Physical Safeguards

In order to protect client privacy, it is important that the following physical safeguards be put in place. For the purposes of this section, authorized persons will be considered only those individuals who have completed Privacy and Security training.

1. Computer Location- A computer used as an ECHO Database workstation must be in a secure location where only authorized persons have access. The workstation must not be accessible to clients, the public, or any other unauthorized participating agency's staff members or volunteers.
  - a. Per Federal Guidelines- All Users are barred from accessing the ECHO Database from a public WiFi connection such as a coffee shop or airport

2. Printer Location- Documents printed from ECHO Database must be sent to a printer in a secure location where only authorized persons have access.
3. PC Access (visual)- Non-authorized persons should not be able to see an ECHO Database workstation screen. Monitors should be turned away from the public or other unauthorized Partner Agency staff members or volunteers and utilize visibility filters to protect client privacy, such as privacy screens

#### **4.9.2 Technical Safeguards**

##### **Workstation Security**

1. The participating agency security officer will confirm that any workstation accessing ECHO Database shall have antivirus software with current virus definitions and frequent full system checks/scans. This may be verified through the agency's technical department
2. The participating agency security officer will confirm that any workstation accessing ECHO Database has, and uses, a hardware or software firewall. This may be verified through the agency's technical department
3. The participating agency must ensure that devices used to access the ECHO Database are password protected with automatic system lock out after user inactivity
4. The participating agency must ensure that the internet connection(s) used to access the ECHO Database from their facilities is set up using network security protocols to prevent unauthorized access to the network and to ECHO Database data saved locally
5. Due to the confidential nature of data stored within the ECHO Database, the system must be accessed from a sufficiently private physical location so as to ensure that persons who are not authorized users of the ECHO Database are not able to view client level data

##### **Establishing ECHO Database User IDs and Access Levels**

1. The participating agency Technical Administrator is responsible for ensuring that all agency End Users have completed mandatory trainings, including ECHO Database Privacy and Security training, along with the End User Responsibilities and Workflow training, prior to being provided with a User ID to access the ECHO Database
2. The participating agency Technical Administrator will ensure all users are up to date with ECHO Database Security Awareness Agreements
3. All End Users will be issued a unique User ID and temporary Password to initially access the system(s), then they will need to create their own password. Sharing of User IDs and passwords by, or among more than one, End User is expressly prohibited. Each End User must be specifically identified as the sole holder of a User ID and Password. User IDs and Passwords may not be transferred from one user to another.
4. The ECHO will always attempt to assign the most restrictive access that allows the End User to efficiently and effectively perform their assigned duties

5. The ECHO will create the new User ID and notify the User ID owner of the temporary password during training.
6. When the participating agency Technical Administrator determines that it is necessary to change a user's access level, the contributory Agency Technical Administrator will notify that CoC's ECHO Database team via email so the the ECHO Database team may update user account as necessary

#### **Passwords**

1. Temporary passwords must be changed on first use. User-specified passwords will be required to comply with the applicable systems' password requirements including login attempts/password disabling, and timed password changes
2. The ECHO Database requires a password change every sixty (60) days
3. End Users must immediately notify their participating agency's technical administrator and the CoC's database administrator if they have reason to believe that someone else has gained access to their password
4. Password resets can be accomplished by using the "forgot password" feature of the applicable system
5. No user shall save their ECHO Database password to their computer or internet browser
6. System users must not store their password in locations that are easily accessible to others (e.g. under the computer keyboard, or posted near their workstation)

#### **Rescinding User Access**

1. End User access should be terminated by the ECHO Database administrator within 24 hours if an End User no longer requires access to perform their duties due to a change of job duties or termination of employment.
2. The contributory agency's security officer must notify the ECHO Database administrator immediately via email of any end user job duties change or end user termination
3. The ECHO Database administrator reserves the right to terminate End User accounts that are inactive for 90 days or more
4. The agency's security officer must submit an email request on behalf of a user whose account has been disabled due to inactivity, the officer wishes to reactivate their account
5. In the event of suspected or demonstrated noncompliance by an End User with the ECHO Database Security Awareness Agreement, or any other ECHO Database plans, policies, or procedures, the Agency Technical Administrator/Contributory Agency security officer should notify the ECHO Database administrator via email to deactivate the User ID for the End User in question until an internal agency investigation has been completed. The ECHO shall be notified of any substantiated incidents that may have resulted in a breach of ECHO Database security and/or client confidentiality, and whether or not a breach is definitively known to have occurred

6. The ECHO Database administrator is empowered to deactivate User IDs pending further investigation of an End User's noncompliance with the ECHO Database Memorandum of Understanding (MOU) is suspected or demonstrated
7. The CoC is empowered to permanently revoke an Agency's access to ECHO Database for substantiated noncompliance with the provisions of these Security Standards, ECHO Database Policies and Procedures, or Privacy Notice that resulted in a release of Protected Health Information (PHI) which also encompasses Personally Identifiable Information (PII) and Personal Protected Information (PPI)
8. For accounts not accessed in and/or deactivated for 180 days or more, the End User will need to go through new User Training after a request has been made by the agency's database contact to the ECHO Database administrator

## **4.10 Agency-Specific Data Security Policies and Procedures**

- The participating agency may develop agency-specific policies and procedures that go beyond the standard policies included in this document
- The participating agency is responsible for ensuring compliance with any agency-specific data security policies and procedures

# **5. Privacy Policies**

## **5.1 Purpose**

These privacy policies are meant to establish limitations on the collection, purpose, and use of data. It defines allowable uses and disclosures, including standards for openness, access, correction, and accountability. The policies provide protections for victims of domestic violence, dating violence, sexual assault, and stalking.

## **5.2 Privacy Notice**

- ECHO will make the privacy notice available to any individual upon request
- The participating agency must post a copy of the privacy notice at each workstation where client data is gathered and entered
- The participating agency must also post a Spanish Translation of the privacy notice

- Outreach workers must inform clients about the privacy notice and provide a copy, if requested
- The participating agency must provide a copy of these privacy policies to anyone who requests them.
- ECHO will ensure that contact information is provided on the privacy notice for the purposes of seeking additional information or submitting complaints

## 5.3 Purpose and Use Limitations

The participating agency and ECHO may only collect and use ECHO Database data for the specific internal purposes relevant to the work of the CoC, as defined in this section.

Every agency with access to Personally Identifiable Information (PII) must implement procedures to ensure and monitor its compliance with privacy policies and may only collect information by lawful and fair means with the knowledge and consent of the individual.

### **Authorized Uses of ECHO Database Data:**

- To provide or coordinate services
- To locate programs that may be able to assist clients
- To produce agency level reports regarding use of services
- To track agency level and CoC system-level outcomes
- For agency operational purposes, including administrative functions such as legal, audits, personnel, oversight, and management functions
- To comply with government and other funding agency reporting requirements
- To identify service needs in our community
- To support CoC system level planning
- To conduct research for government and educational purposes
- To monitor compliance with ECHO Database policies and procedures
- To accomplish any and all other purposes deemed necessary by the CoC Board

## 5.4 Participating Agency Data Sharing

All client information entered in ECHO Database by the participating agency is shared with the agency's system users and with the ECHO Database Lead. This ensures streamlined access for the participating agency's internal purposes and for oversight by the lead agency responsible for maintaining the ECHO system.

### **5.4.1 Interagency Data Sharing / Client Consent**

- With explicit client consent – an ROI (Release of Information) – all client information is shared with system users at other participating agencies for authorized uses
  - No client can be denied services for refusing consent to share their data or for refusing to have their data entered
  - The consent for data sharing must be informed, voluntary, and clearly documented via an ROI that is uploaded to the ECHO database.
  - Clients can revoke consent in writing at any time, and such revocation must be honored with no impact on the services they receive
- The Executive Director, Program Director, or an equivalent senior leader of each participating agency is ultimately responsible for ensuring their agency's compliance with the Interagency Data Sharing Policy.
  - This includes ensuring proper training for staff on the data sharing protocols, safeguarding client confidentiality, and ensuring that data sharing practices align with applicable legal and ethical standards.
- For any agency designated as a domestic violence or human trafficking-specific service provider that is not funded by the Violence Against Women Act (VAWA) or other federal or state funding and is not otherwise restricted from using a shared database, the agency will have partitioned access to client data within the ECHO Database. This means that data visibility will be limited to the agency's view only, preventing access to data that may be sensitive or irrelevant to other agencies.
- The above mentioned partitioning will also apply to agencies that have specialized restrictions on their use of shared databases in order to ensure that sensitive information, particularly that related to vulnerable populations such as survivors of domestic violence or human trafficking, is protected in accordance with applicable regulations and policies.
- Compliance with this policy will be regularly monitored by the HMIS Lead Agency and participating agencies to ensure proper implementation. Reviews of data sharing practices and client consent procedures will be conducted annually, or as needed, to ensure that data sharing remains in compliance with changing laws, regulations, and client needs.

#### **5.4.2 External Entity Data Sharing**

At times, it may be necessary for participating agencies to report or share the information they have collected in the Database with other participating agencies or other outside entities.

To ensure data security and client confidentiality, the following conditions must be met and strictly adhered to when sharing data with entities external to the participating agency:

1. All data sharing must align with the limitations and conditions set forth in **Section 5.3** and the Privacy Notice in **Appendix I**

2. Any and all data shared externally must be fully anonymized. Personally identifiable client information (PII) must be removed from the dataset prior to sharing. For the purpose of data sharing, PII includes, but is not limited to, the following:
  - a. Full names or initials
  - b. Exact Age (sharing age ranges is acceptable)
  - c. Birth year, month, or day
  - d. Any other information that could be used to identify an individual, either directly or when combined with other data
3. The reporting agency may only report or share data that it has entered itself or that is specifically linked to its own operations
4. In addition to PII, any data that identifies another agency – such as the agency’s name, address, phone number, or other identifying details – must be excluded from shared datasets
5. The entity sharing the data is solely responsible for ensuring the confidentiality of client information during the sharing and reporting process. Any breach of confidentiality will be the responsibility of the sharing entity

#### **5.4.3 Approval for research and community-level reporting**

Any data sharing for external research purposes or community-level/system wide reporting requires prior written approval from the CoC and Lead Agency. A formal request must be submitted and approved before any such data can be shared with outside entities.

**Refer to the “CoC Policies & Procedures for Requests of Letters of Support, MOUs, & HMIS Data” for more information on research and community reporting**

### **5.5. Data Requests**

**For any entity** (database participating and non participating entities) who wishes to request data from the system, a formal request to the CoC and ECHO is required. Refer to the “CoC Policies & Procedures for Requests for Letters of Support, MOUs, & HMIS data” for details and process.

### **5.6 Client Consent**

- The participating agency may infer client consent to collect and enter information into ECHO Database from any person who seeks or receives assistance from the agency **provided the Privacy Policy Notice is posted conspicuously and reviewed with the client prior to data entry**

- All information entered into the ECHO Database is shared between the agency's system users and with ECHO, based on the inferred client consent
- The agency must seek and obtain client consent using the release of information (ROI) form in order to share information with other participating agencies if there is no current ROI in the Database.
  - If there is an existing, valid ROI, the agency need only verify the ROI in the database in order to share across agencies
- When clients consent to share information, system users at other participating agencies will have access to the client's record and case history for authorized uses
- Informed client consent is valid until such time as the client revokes consent
- Clients who have consented to share information with other participating agencies through an ROI may revoke consent in writing at any time
- The participating agency must upload copies of consent documentation to the client's case file in the database and mark the client's record as having given or refused consent
- Should a client refuse consent to share or have their data entered, they can not be refused services by any participating agency

#### **Procedures (Initial Consent)**

1. Personnel from the participating agency will notify the client that the information they collect will be entered into the ECHO Database and will explain the purposes for collecting information in the ECHO Database via a review of the privacy notice
2. Personnel from the participating agency will explain the Release of information form, and the client's right to revoke data sharing in writing at any time
3. For families, an adult client can provide consent on behalf of underage household members by listing them in the spaces provided on the form. Additionally, the participating agency must seek consent separately from each adult in the household. A legal guardian (or another adult, if a guardian is not present) may sign on behalf of minors in the household
4. The client will be provided the ROI for review, will be explained its content, and will be asked to complete it
  - a. Should a **client decline the ROI**, information can still be entered into the database; however, the information cannot be shared outside of the agency
    - i. The client's declination should be noted in the client's database profile in the appropriate area
  - b. Should a client refuse to have their information entered into the ECHO Database at all, agency staff should collect information via paper in accordance with their own requirements and an anonymized record entered into the Database

5. The signed, physical ROI should be scanned and uploaded to the ECHO Database in the client's ROI record
  - a. The physical ROI should be stored securely on site at the entering agency in accordance with the entering agency's own record keeping policies or destroyed
6. Digital consent is not accepted at this time

### **Procedures (Subsequent Consent)**

#### **For clients previously entered into the database:**

1. Personnel from the participating agency will check to see if a client's file is available in the database
  - a. If client file does not exist, follow consent procedures for "initial consent"
2. If located, the client file should be checked for an existing ROI
  - a. If an existing ROI is not in place, the client should be given the option to sign one
3. Verify the ROI that was uploaded to the database
  - a. Check names of minor family members and verify date signed
4. If the ROI is valid, mark the client's case file as having an ROI verified from a separate institution

# Appendix I Privacy Notice (English & Spanish)

## HMIS/SERVICE PROVIDER PRIVACY NOTICE

This notice applies to all service providers who utilize the ECHO West Texas Database, also known as HMIS, and addresses how information about clients may be used and disclosed as well as client rights over their information. This notice may be amended at any time, and amendments may affect information obtained before the date of the amendment.

### **Data Collection & Purpose**

The Homeless Management Information System (HMIS) is an information gathering system used to collect data on housing and services provided to homeless individuals and families as well as information on persons at risk of homelessness. Participating providers are required to collect universal data elements from all clients, including personally identifiable information (PII), demographic information, and housing history. This information is used to better understand the extent and nature of homelessness in Lubbock County, evaluate effectiveness of agency responses, and improve future housing and service provisions. Some providers are required by their funders to obtain certain additional information to assess services, determine eligibility, and monitor outcomes. Most federally funded homelessness programs require client information to be recorded in an HMIS database. The ECHO database has strict privacy measures and policies in place to ensure security of client information. We only collect information deemed appropriate and necessary for program operation or information that is required by law or required by funders of this site. We do not need your consent to enter a record of your visit into the HMIS; however, you may refuse to have your personal identifying information within said record and still be eligible to receive services.

If you have any questions or concerns about the information provided, please speak to an intake worker.

### **Permitted Data Uses and Disclosures**

All HMIS participating agencies are held to strict federal, state, and local standards when it comes to the confidentiality of PII ('Personally Identifying Information', any information that can be used to identify an individual such as date of birth, social security number, client name). There are limitations to how your information can be used after collection and how it can be shared:

#### Required uses and disclosures:

1. Client must have access to their information; and
2. Disclosures for oversight of compliance with HMIS privacy and security standards.

#### Permitted uses and disclosures:

3. To provide and/or coordinate services to an individual or family;
4. For functions related to payment or reimbursement for services;
5. To carry out administrative functions, including but not limited to legal, audit, personnel, oversight and management functions;
6. For creating de-identified reporting from PII;
7. Uses and disclosures required by law;
8. Uses and disclosures to avert a serious threat to health or safety;
9. Uses and disclosures about victims of abuse, neglect or domestic violence;
10. Uses and disclosures for research purposes;
11. Uses and disclosure for law enforcement purposes;

Some providers may have more restrictive privacy policies which can be obtained upon request from such providers.

### **Client Control Over Data:**

We recognize every person as the owner of all information about themselves, and any parent, legal guardian, or legal power of attorney can be the designated owner of all information about any minor household members under their guardianship; however, minors retain the right to revoke consent at any time and/or to refuse to have their data collected. By seeking assistance from the HMIS provider and consenting to your personal information being entered into a record to us, you transfer responsibility of your HMIS record to us, and we are responsible for handling your record in accordance with HMIS privacy policies and any applicable federal, state, or local requirements.

Any client request for privacy will not result in exclusion from services.

### **Client Rights:**

- You retain the right to ownership of your information within the HMIS
- You retain the right to revoke consent at any time and have your data removed from the HMIS
- You have the right to refuse to answer any question you do not feel comfortable answering and not have it recorded in the HMIS
- You have the right to view and correct any information gathered within the HMIS upon request
- You have the right to ask questions or submit grievances to your provider regarding privacy and security policies and practices
- You have the right to an anonymized record within the HMIS with a request from this service provider
- You have the right to choose if your information is shared outside of this agency and/or with outside researchers and other providers outside of the HMIS; NOTE: a decision not to share data does not prohibit this project from entering your data into HMIS. It only prohibits your information from being shared in accordance with your wishes.

**If you do not understand any of the information within this form, you may ask your intake worker for further explanation or an alternative format. You can receive a copy of any and all HMIS policies and procedures from your intake worker.**

## AVISO DE PRIVACIDAD DE HMIS/PROVEEDOR DE SERVICIOS

Este aviso se aplica a todos los proveedores de servicios que utilizan la base de datos de ECHO West Texas, también conocida como HMIS, y aborda cómo se puede usar y divulgar la información sobre los clientes, así como los derechos de los clientes sobre su información. Este aviso puede ser modificado en cualquier momento, y las enmiendas pueden afectar la información obtenida antes de la fecha de la enmienda.

### **Recopilación de datos y finalidad**

El Sistema de Información para la Gestión de las Personas sin Hogar (HMIS, por sus siglas en inglés) es un sistema de recopilación de información que se utiliza para recopilar datos sobre la vivienda y los servicios prestados a las personas y familias sin hogar, así como información sobre las personas en riesgo de quedarse sin hogar. Los proveedores participantes deben recopilar elementos de datos universales de todos los clientes, incluida la información de identificación personal (PII), la información demográfica y el historial de vivienda. Esta información se utiliza para comprender mejor el alcance y la naturaleza de la falta de vivienda en el condado de Lubbock, evaluar la efectividad de las respuestas de la agencia y mejorar las futuras proporciones de vivienda y servicios. Algunos proveedores son requeridos por sus financiadores para obtener cierta información adicional para evaluar los servicios, determinar la elegibilidad y monitorear los resultados. La mayoría de los programas para personas sin hogar financiados por el gobierno federal requieren que la información del cliente se registre en una base de datos de HMIS. La base de datos de ECHO cuenta con estrictas medidas y políticas de privacidad para garantizar la seguridad de la información de los clientes. Sólo recopilamos la información que se considera apropiada y necesaria para el funcionamiento del programa o la información que es requerida por la ley o requerida por los financiadores de este sitio. No necesitamos su consentimiento para ingresar un registro de su visita en el HMIS; Sin embargo, puede negarse a tener su información de identificación personal dentro de dicho registro y aún ser elegible para recibir servicios.

Si tiene alguna pregunta o inquietud sobre la información proporcionada, hable con un trabajador de admisión.

### **Usos y divulgaciones de datos permitidos**

Todas las agencias participantes de HMIS están sujetas a estrictos estándares federales, estatales y locales en lo que respecta a la confidencialidad de la PII ('Información de identificación personal', cualquier información que pueda usarse para identificar a un individuo, como la fecha de nacimiento, el número de seguro social, el nombre del cliente). Existen limitaciones en cuanto a cómo se puede usar su información después de la recopilación y cómo se puede compartir:

#### Usos y divulgaciones requeridos:

1. El cliente debe tener acceso a su información; y
2. Divulgaciones para la supervisión del cumplimiento de los estándares de privacidad y seguridad de HMIS.

#### Usos y divulgaciones permitidos:

3. Para proporcionar y/o coordinar servicios a una persona o familia;
4. Para funciones relacionadas con el pago o reembolso de servicios;
5. Para llevar a cabo funciones administrativas, incluidas, entre otras, las funciones legales, de auditoría, de personal, de supervisión y de gestión;
6. Para crear informes anónimos a partir de PII;
7. Usos y divulgaciones requeridos por la ley;
8. Usos y divulgaciones para evitar una amenaza grave para la salud o la seguridad;
9. Usos y divulgaciones sobre víctimas de abuso, negligencia o violencia doméstica;
10. Usos y divulgaciones con fines de investigación;
11. Usos y divulgación con fines de aplicación de la ley;

Algunos proveedores pueden tener políticas de privacidad más restrictivas que se pueden obtener a pedido de dichos proveedores.

### **Control del cliente sobre los datos:**

Reconocemos a cada adulto legal como el propietario de toda la información sobre sí mismo, y a cualquier padre, tutor legal o poder legal como el propietario designado de toda la información sobre cualquier miembro del hogar bajo su tutela. Al buscar ayuda del proveedor de HMIS y dar su consentimiento para que su información personal se ingrese en un registro, usted nos transfiere la responsabilidad de su registro de HMIS, y somos responsables de manejar su registro de acuerdo con las políticas de privacidad de HMIS y cualquier requisito federal, estatal o local aplicable.

### **Derechos del cliente:**

- Usted conserva el derecho a la propiedad de su información dentro del HMIS
- Tiene derecho a negarse a responder cualquier pregunta que no se sienta cómodo respondiendo y a que no quede registrada en el HMIS
- Tiene derecho a ver y corregir cualquier información recopilada en el HMIS si lo solicita ➤ Tiene derecho a hacer preguntas o presentar quejas a su proveedor con respecto a las políticas y prácticas de privacidad y seguridad
- Tiene derecho a un registro anónimo dentro del HMIS con una solicitud de este proveedor de servicios ➤ Usted tiene derecho a elegir si su información se comparte fuera de esta agencia y/o con investigadores externos y otros proveedores fuera de la HMIS; NOTA: la decisión de no compartir datos no prohíbe que este proyecto ingrese sus datos en HMIS. Solo prohíbe que su información se comparta de acuerdo con sus deseos.

**Si no comprende la información contenida en este formulario, puede pedirle a su trabajador de admisión una explicación más detallada o un formato alternativo. Puede recibir una copia de todas y cada una de las políticas y procedimientos de HMIS de su trabajador de admisión.**

# Appendix II Client Release of Information (ROI) (English & Spanish)

## Client Release of Information for the ECHO West Texas HMIS/Database

To give you the best service, we need to collect some information for our database. This safe and private database is managed by trained staff. It helps service providers work together to make sure you get the help you need on time. The database also helps the Lubbock community keep track of how many people are homeless or at risk of homelessness.

We need to collect some personal information to improve our services, plan new ones, and work with other service providers. With this form, you can choose to allow your information to be shared with these providers.

By agreeing, I understand that my information will be entered into the ECHO West Texas database. I confirm that the information I give is correct. I understand that local service providers may share this information to help connect me with services.

I know that the information in the database may be used by service providers and ECHO West Texas for things like research, reports on homelessness, housing programs, and other services. I agree to allow my personal information to be collected and shared with service providers in the database. If I no longer want my information collected or shared, I can stop it by contacting the agency or ECHO West Texas in writing. Any information shared before I stop cannot be taken back.

A representative has answered my privacy questions and explained the Privacy Notice. By signing this form, I agree to the terms and conditions listed above.

---

Client Name [Print]	Date	Client Signature	Date
---------------------	------	------------------	------

---

Authorized Agency Representative [Print]	Date	Authorized Signature	Date
--	------	----------------------	------

**Client Consent on Behalf of Household Members**

An adult head of household may provide consent on behalf of minor family members to share their information in the HMIS/Database.

\_\_\_\_\_  
Family Member Name 1  
[Print]

\_\_\_\_\_  
Head of Household  
[Initials]

\_\_\_\_\_  
Family Member Name 2  
[Print]

\_\_\_\_\_  
Head of Household  
[Initials]

\_\_\_\_\_  
Family Member Name 3  
[Print]

\_\_\_\_\_  
Head of Household  
[Initials]

\_\_\_\_\_  
Family Member Name 4  
[Print]

\_\_\_\_\_  
Head of Household  
[Initials]

\_\_\_\_\_  
Family Member Name 5  
[Print]

\_\_\_\_\_  
Head of Household  
[Initials]

\_\_\_\_\_  
Family Member Name 6  
[Print]

\_\_\_\_\_  
Head of Household  
[Initials]

\_\_\_\_\_  
Family Member Name 7  
[Print]

\_\_\_\_\_  
Head of Household  
[Initials]

**Divulgación de información al cliente**  
para la base de datos/HMIS ECHO West Texas

Para brindarle el mejor servicio, necesitamos recopilar cierta información para nuestra base de datos. Esta base de datos segura y privada es administrada por personal capacitado. Ayuda a los proveedores de servicios a trabajar juntos para asegurarse de que reciba la ayuda que necesita a tiempo. La base de datos también ayuda a la comunidad de Lubbock a realizar un seguimiento de cuántas personas están sin hogar o en riesgo de quedarse sin hogar.

Necesitamos recopilar cierta información personal para mejorar nuestros servicios, planificar otros nuevos y trabajar con otros proveedores de servicios. Con este formulario, puede optar por permitir que su información se comparta con estos proveedores.

Al aceptar, entiendo que mi información será ingresada a la base de datos de ECHO West Texas. Confirmó que la información que doy es correcta. Entiendo que los proveedores de servicios locales pueden compartir esta información para ayudarme a conectarme con los servicios.

Sé que la información en la base de datos puede ser utilizada por los proveedores de servicios y ECHO West Texas para cosas como investigaciones, informes sobre personas sin hogar, programas de vivienda y otros servicios. Acepto permitir que mi información personal sea recopilada y compartida con los proveedores de servicios en la base de datos. Si ya no quiero que se recopile o comparta mi información, puedo detenerlo comunicándome con la agencia o con ECHO West Texas por escrito. Cualquier información compartida antes de que me detenga no se puede recuperar.

Un representante ha respondido a mis preguntas sobre privacidad y ha explicado el Aviso de privacidad. Al firmar este formulario, acepto los términos y condiciones enumerados anteriormente.

---

Nombre del cliente [Imprimir]	Fecha	Firma Clint	Fecha
-------------------------------	-------	-------------	-------

---

Agencia Autorizada Representante [Imprimir]	Fecha	Firma Autorizada	Fecha
--	-------	------------------	-------

### Consentimiento del cliente en nombre de los miembros del hogar

Un cabeza de familia adulto puede dar su consentimiento en nombre de los miembros menores de edad de la familia para compartir su información en la base de datos de HMIS.

---

Nombre del miembro de la familia 1  
[Imprimir]

---

Jefe de familia  
[Iniciales]

---

Nombre del miembro de la familia 2  
[Imprimir]

---

Jefe de familia  
[Iniciales]

---

Nombre del miembro de la familia 3  
[Imprimir]

---

Jefe de familia  
[Iniciales]

---

Nombre del miembro de la familia 4  
[Imprimir]

---

Jefe de familia  
[Iniciales]

---

Nombre del miembro de la familia 5  
[Imprimir]

---

Jefe de familia  
[Iniciales]

---

Nombre del miembro de la familia 6  
[Imprimir]

---

Jefe de familia  
[Iniciales]

---

Nombre del miembro de la familia 7  
[Imprimir]

---

Jefe de familia  
[Iniciales]

# Appendix III Security Self Audit

Applicable to any HMIS/Database participating agency

Agreements, Certifications, and Licenses		
	Signed HMIS CHO (agency) MOU	Confirm agency has a current signed copy of this document
	Signed User MOUs	Conduct spot check on 5+ of active HMIS users to confirm you have these documents (for agencies with 50+ users, sample 10% of them)
	Reviewed the ECHO West Texas Security Policies in the HMIS/Database Policies & Procedures	Confirm your agency has reviewed these policies
	HMIS Contact	Please provide us with at least one individual who is your lead HMIS contact
	Agency Security Officer	Please provide us with at least one lead person who knows your agency's security efforts

Privacy Notice		
	Privacy notice (spanish & english versions) posted publicly for client or public viewing	This notice should be posted in your lobby and/or intake offices in each data collection location. Field staff should carry a copy
	Locations of postings	Give a brief description of location of notice(s), include addresses where appropriate
	Notice awareness	Confirm that agency staff have read and understand the notice
	Additional privacy notices	Provide copies of any additional privacy notices used at site
	Clients presented with Privacy Notice at intake	Confirm your agency reviews the Privacy Notice with any new clients during intake
	Privacy Notice made available upon request	Confirm there are extra copies of this document for clients or have the ability to print copies upon request

Hard Copy Data		
	Protect hard copy data from unauthorized viewing or access	Ensure client files are not left unattended when not in use and their names are not in plain sight of non-essential personnel
	Files are locked in a drawer or cabinet	Complete a spot check of areas where files are located to make sure drawers are locked
	Offices are locked when not occupied	Complete spot check of both individual offices and main offices to make sure they are locked
	No visible client files or reports on unoccupied desks or workspaces	Complete spot check of all unoccupied desks and/or offices
	Printer location(s)	Ensure any printers used to print client information located in locked office or out of public/client access

Computer Systems		
	Virus Protection with automatic updates	Ensure all computers have automatic updates for their virus protection
	Virus software name, version, last update	Provide us with the name of your anti-virus software, software version, last update date
	Operating System (OS) updates	Make sure all computers, tablets, and mobile devices have automatic updates for their operating system.

Physical Access		
	Workstations in secured locations (locked offices)	Complete a spot check on at least 10% of workstations
	Workstations are logged off when not in use	Complete a spot check on at least 10% of workstations
	Workstations are password protected	Complete a spot check on at least 10% of workstations
	Workstations are never connected to an open Wi-Fi network (e.g. internet cafe, library, airport, etc.)	Complete a spot check on 10% of workstations and/or interview 10% of staff to ensure compliance
	Written plan for remote access/work	Ensure agency has a plan for remote access/work if applicable
	Login Credentials not stored on or near workstation (i.e. under keyboard)	Complete a spot check on at least 10% of workstations
	Confirm active HMIS users are still employed by agency	Ensure no terminated employees still have access to the system
	Workstation screens turned away from public/unauthorized viewing	Complete a spot check of at least 10% of workstations
	Login Credentials not shared	Interview at least 5 staff with access to ensure compliance

# Appendix IV Community Database Free License Application Form

## 1. Organization Information

- Organization Name: \_\_\_\_\_
- Organization Type (Non-Profit/Charity/Community-Based): \_\_\_\_\_
- Registration Number (if applicable): \_\_\_\_\_
- Address: \_\_\_\_\_
- Website: \_\_\_\_\_
- Director/Equivalent Name: \_\_\_\_\_
- Director Email: \_\_\_\_\_
- Director Phone: \_\_\_\_\_

## 2. Mission and Alignment

- Briefly describe your organization's mission and primary activities:  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_
- How does your organization's mission align with the goals of the Community Database?  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

## 3. Financial Need

- Please explain why your organization requires a free license and cannot afford the full cost:  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

**4. Intended Use of the Community Database**

- Describe how your organization intends to use the Community Database:

---

---

---

- Who will benefit from your use of the database? (e.g., underserved communities, research initiatives, etc.)

---

---

---

**5. Compliance and Commitment**

- Does your organization agree to comply with all data privacy and usage policies? (Yes/No): \_\_\_\_\_
- Will your organization use the database for non-commercial purposes only? (Yes/No): \_\_\_\_\_
- Can your organization provide periodic reports on the impact of the database usage? (Yes/No): \_\_\_\_\_

**6. Supporting Documentation** Please attach the following documents:

- Proof of non-profit status (e.g., tax-exempt certificate or equivalent)
- A statement of financial need
- A letter of commitment to adhere to data privacy and usage policies

**7. Declaration** I, \_\_\_\_\_, certify that the information provided in this application is accurate and that our organization agrees to abide by the terms and conditions set forth in the License Allocation Policy.

Signature: \_\_\_\_\_

Date: \_\_\_\_\_

**Submission Instructions** Please submit the completed application and supporting documents to ECHO West Texas. For any questions, contact the ECHO Database Admin Team at [data@echowtx.org](mailto:data@echowtx.org).