

El Paso CoC TX-603

Homeless Management Information
System (HMIS)
Policies and Procedures



El Paso Coalition for the Homeless (EPCH)

EPCH is the HMIS lead for the El Paso City & County Continuum of Care.

6044 Gateway East, Suite 211, El Paso, TX 79905

Tel: (915) 843-2170

Fax: (915) 843-2184

HMIS Contact Information		
Team	Contact Email	Reason
HMIS Administrator	ggray.epch@elp.twcbc.com	<ul style="list-style-type: none"> ▪ General technical support for HMIS issues related to user access, troubleshooting, information requests, system functionality errors, etc. ▪ Training ▪ Requests for issues related to data quality, management and/or mandated reports, report failure, etc. <p>Requests for issues related mandated reports, report failure, etc.</p>
HMIS Support	Dherald.epch@elp.twcbc.com	<p>General technical support for HMIS matters related to user access, troubleshooting, information requests, system functionality errors, etc.</p>

PROJECT SUMMARY

Background

To end homelessness, a community must know the scope of the problem, the characteristics of those who find themselves homeless, and understand what is working in their community and what is not. Reliable data enables a community to work confidently towards their goals as they measure outputs, outcomes, and impacts.

A Homeless Management Information System (HMIS) is the information system designated by the Continuum of Care (CoC) to comply with the requirements of CoC Program Interim Rule 24 CFR 578. It is a locally-administered data system used to record and analyze client, service and housing data for individuals and families who are homeless or at risk of homelessness. HMIS is a valuable resource because of its capacity to integrate and unduplicated data across projects in a community. Aggregate HMIS data can be used to understand the size, characteristics, and needs of the homeless population at multiple levels: project, system, local, state, and national.

The Annual Homeless Assessment Report (AHAR) is HUD's annual report that provides Congress with detailed data on individuals and households experiencing homelessness across the country each year. This report could not be written if communities were not able to provide HUD with reliable, aggregate data on the clients they serve.

In 2010 the U.S. Interagency Council on Homelessness (USICH) affirmed HMIS as the official method of measuring outcomes in its Opening Doors: Federal Strategic Plan to Prevent and End Homelessness. Through that effort, other federal programs that serve people experiencing homelessness populations are now required to coordinate their efforts with HUD.

HMIS is now used by the federal partners and their respective programs in the effort to end Homelessness, which includes:

- U.S. Department of Health and Human Services (HHS)
- U.S. Department of Housing and Urban Development (HUD)
- U.S. Department of Veterans Affairs (VA)

Programs that receive other sources of funding are not required to participate in the HMIS, but they are strongly encouraged to participate to contribute to a more comprehensive understanding of homelessness in the region.

The HMIS Data Manual and the HMIS Data Dictionary <https://files.hudexchange.info/resources/documents/HMIS-Data-Dictionary.pdf> are updated periodically and provide communities with baseline data collection requirements developed by each of these federal partners. EPCH HMIS is a response to the HUD mandated implementation of an HMIS database. The EPCH HMIS is an online database used by organizations that provide services to persons experiencing homelessness or are at-risk of homelessness.

It records demographic and service usage data and produces an unduplicated count of the people using those services.

The EPCH HMIS implementation is led by the El Paso Coalition for the Homeless, as determined by and with oversight from the CoC Board. As such, the CoC Board shall be the final authority for certifying the participation status for all organizations, when applicable. Any organization appealing the CoC Board's determination will submit a written request for review within five (5) days of notification of Non-participation.

Mission Statement

The EPCH HMIS will use HMIS to advance the provision of quality services for persons who are homeless or at-risk of homelessness, to improve data collection and promote more responsive policies to prevent and end homelessness in El Paso City & County.

Vision

The EPCH HMIS is dedicated to providing the best possible, highest quality regional HMIS to enhance the delivery of services for persons experiencing homelessness or at risk of homelessness. Specifically, HMIS will:

- Facilitate the coordination of service delivery.
- Enable agencies to track referrals and services provided, report outcomes, and manage client data using an accessible, user-friendly and secure technology.
- Enhance the ability of policy makers and advocates to gauge the extent of homelessness and plan services appropriately throughout our region.

olicies and Procedures

EPCH HMIS Software

EPCH HMIS is a comprehensive case management system that allows Users to use the collected information to make informed policy and programmatic decisions. It also includes a focus on outcomes management, allowing the user to set and measure client and program milestones and achievements.

EPCH HMIS includes the following components:

- Advanced security features
- Bed tracking and assignment feature
- Client demographic data collection
- Comprehensive client case management
- Coordinated entry
- Customized assessment capability
- Customized reporting capability
- Employment, education, and housing history tracking
- Group case notes/services management
- Information and referral capabilities
- Outcome management
- Outreach
- Real-time data collection and reporting

1. ROLES AND RESPONSIBILITIES

1.1 EPCH HMIS Responsibilities

Policy:

Policy:

The EPCH will be responsible for the organization and management of the HMIS as determined by and with oversight from the CoC Board.

Responsibilities:

The EPCH is responsible for all system-wide policies, procedures, communication, and coordination. It is also the exclusive contact with the HMIS vendor, and with its help, will implement all necessary system-wide changes and updates.

Procedure:

- HMIS Administrators are the primary positions at EPCH for HMIS management.

1.2 HMIS Administrator Responsibilities

Policy:

HMIS Administrators will provide training and technical support to Participating Organizations.

Responsibilities:

The HMIS Administrator is responsible for:

- Providing training support to Participating Organizations by determining training needs of Users, developing training materials, and training Users in equipment and software;
- Providing technical support to Participating Organizations;
- Managing user accounts and access control;
- Identifying and developing system enhancements and communicating changes to Participating Organizations;
- Monitor Data Quality standards;
- Communicating system-related information to Participating Organizations; and
- Developing and modifying reports for Users

Procedure:

- The El Paso CoC is the designated HMIS Administrator.

1.3 Organization Administrator Responsibilities

Policy:

Each Participating Organization must designate an Organization Administrator and a backup Organization Administrator responsible for the oversight of all personnel that generate or have access to client data in the EPCH HMIS to ensure adherence to the

Policies & Procedures described in this document.

Responsibilities:

The Organization Administrator is responsible for:

- Notifying the HMIS Administrator of personnel changes within three (3) business days;
- Monitoring compliance with standards of confidentiality and data collection, entry, and retrieval;
- Ensuring that all authorized Users adhere to and understand the HMIS User Agreement;
- Ensuring organizational adherence to the Policies & Procedures; and
- Reporting security incidents and violations of the Policies & Procedures to the HMIS Administrator

Procedure:

- Participating Organizations must provide the HMIS Lead Agency the name and contact information of the Organization Administrator and backup Organization Administrator.
- Any changes to that information must be reported to the HMIS Administrator within three (3) business days.

1.4 HMIS Lead Agency Communication with Participating Organizations

Policy:

The HMIS Administrator is responsible for communicating any system-related information to Participating Organizations in a timely manner.

Procedure:

- HMIS Administrators will communicate system-related updates to the Organization Administrator and/or Users through various communication channels, which includes but is not limited to email, meetings and/or website.
- Organization Administrators are responsible for ensuring that all members of their organization are informed of appropriate HMIS related communication.
- Specific communications will be addressed to the person or parties involved.

1.5 Participating Organization Communication with HMIS Lead Agency

Policy:

The Participating Organization is responsible for communicating needs and questions regarding the EPCH HMIS to the HMIS Administrator in a timely manner.

Procedure:

- Participating Organization will send email communication to the HMIS Administrator.
- Specific communications will be addressed to the person or parties involved.
- Participating Organizations must have 75% attendance at monthly HMIS Steering Committee meetings during the calendar year.

2. IMPLEMENTATION POLICIES AND PROCEDURES

2.1 HMIS Organization Agreement Requirement

Policy:

The Executive Director of each Participating Organization shall follow, comply, and enforce the HMIS Participating Organizations Agreement (Appendix A). The Executive Director must sign the HMIS Participating Organization Agreement in advance before Users are granted access to the EPCH HMIS.

Procedure:

- An original, scanned, or a digitally signed HMIS Participating Organizations Agreement must be presented to the HMIS Administrator before program implementation or user training on the EPCH HMIS.
- After HMIS Participating Organizations Agreement is signed, the HMIS Administrator will train Users to use the EPCH HMIS.
- A username and password will be granted to Users after required training is completed.
- New Participating Organizations will be allowed two (2) calendar months to comply with the procedure. Prior to the end of the two month deadline, agencies will be considered participating if they have executed all necessary participation agreements, met any required finance requirements, have at least two employees (or other approved personnel) that are qualified and trained for data entry and have had representation at every regular HMIS Steering Committee Meeting held during the period.

2.2 HMIS User Agreement Requirement

Policy:

Users of any Participating Organizations shall follow, comply, and enforce the HMIS User Agreement (Appendix B). The User must sign an HMIS User Agreement before being granted access to the EPCH HMIS.

Procedure:

- The HMIS User Agreement is accessible within the HMIS and must be signed with initial access to the system.
- The HMIS User Agreement will automatically require re-signing upon each anniversary of the User. Failure to sign will prevent access to the system.

2.3 Data Collection Requirements

Policy:

Participating Organizations will collect and verify the minimum set of data elements for all clients served by their programs.

Procedure:

- Participating Organizations must enter data into the system in compliance with the “timeliness” Data Quality standard described under item 5.1.
- Users must collect all the universal data elements set forth in the most recently approved [HMIS Data Standards](#) as described in the Data Quality standards under item 5.1

The universal data elements include:

- | | |
|---|--|
| <ul style="list-style-type: none"> • Name • Social Security Number • Date of Birth • Race • Ethnicity • Gender • Veteran Status • Disabling Condition | <ul style="list-style-type: none"> • Project Entry Date • Project Exit Date • Destination • Relationship to Head of Household • Client Location • Housing Move-In Date • Living Situation |
|---|--|
- Users must also collect all the program-specific data elements at project entry and exit. The program-specific data elements include:

<ul style="list-style-type: none"> • Income and Sources • Non-Cash Benefits • Health Insurance • Physical Disability • Developmental Disability • Chronic Health Condition • HIV/AIDS • Mental Health Problem 	<ul style="list-style-type: none"> • Substance Abuse • Domestic Violence • Contact • Date of Engagement • Bed-night Date • Housing Assessment Disposition
---	---
 - These standards are already required fields in the EPCH HMIS. For other funder-specific program data elements refer to the most recently approved HMIS Data Standards Manual.
 - Disclaimer: while these are the minimal standard per HUD, the El Paso CoC may have additional data collection requirements.

2.4 Technical and Security Standards

Policy:

Participating Organizations must meet the technical standards outlined below to participate in the EPCH HMIS.

Procedure:

The Clarity Human Services software takes advantage of the latest in web technologies. For both security and compatibility, agency IT Staff should ensure all workstations are outfitted with the latest version of the Web Browser you use.

The following web browsers are supported by Clarity:

- Microsoft Internet Explorer
- Mozilla Firefox
- Google Chrome
- Apple Safari

Connection to the internet is the sole responsibility of the Participating Organizations and is a requirement to participate in the EPCH HMIS. For each user connecting over a given line there must be at least 20 Kbps of bandwidth available for the user. This means that if a given site has 20 users, there would need to be at least 400 Kbps of bandwidth available to access HMIS, taking into account any other traffic that may be using the same connection. Other traffic would include that used by email, web access, and web serving.

- Minimum Hardware Requirements:
- Device hardware must meet or exceed the recommended hardware requirements for the Operating System and web browser.

2.5 Maintenance of Onsite Computer Equipment

Policy:

Participating Organizations will commit to a reasonable program of equipment maintenance to sustain an efficient level of system operation.

Procedure:

The Executive Director (or other empowered officer) will be responsible for the maintenance and disposal of onsite computer equipment. This includes:

- Purchase of and upgrades to all existing and new computer equipment for utilization in the system.
- Workstations accessing the system must have a username/password to log onto Microsoft Windows Operating System.
- Workstation access system must have locking, password-protected screen saver.
- All workstations and computer hardware (including organization network equipment) must be stored in a secure location (locked office area).

2.6 HMIS Technical Support Protocol

Policy:

The HMIS Lead Agency will provide technical support to all Participating Organizations as needed.

Procedure:

Users should seek technical support by contacting the HMIS Help Desk.

- The HMIS Administrator support Hours are Monday through Friday (excluding holidays) from 8:00 am to 5:00 pm.
- The HMIS Administrator will request sufficient issue details to include screenshots, reports, etc., information needed to recreate the problem.
- The HMIS Administrator will try to respond to all email inquiries and issues within three (3) business days, but support load, holidays, and other events may impact response time.
- The HMIS Administrator will submit a ticket to vendor if the issue cannot be resolved by the HMIS Administrator.

2.7 System Availability

Policy:

The EPCH HMIS will be available to Users during business hours only except during agency approved holidays and when all HMIS staff is in attendance at EPCH meetings requiring their participation. The vendor and the HMIS Lead Agency will inform Users in advance of any planned interruption in service.

Procedure:

- The vendor will communicate to the EPCH HMIS of any necessary downtime for system upgrades and patches. These will be performed outside of business hours when possible.
- If it is determined that the EPCH HMIS accessibility is disabled system-wide, the HMIS Administrators will analyze and determine the problem.
- The HMIS Administrator will work with the software vendor to repair the problem.
- The HMIS Administrators will send email communication to the /User within two (2) hours of issue discovery and inform them of anticipated interruptions to system availability.

2.8 Participation and Other Fees

Policy:

EPCH reserves the right to charge a fees for system use and customized reporting.

Procedure:

- Consult HMIS Lead Agency regarding fees if needed.
- Participation Fees may be required to cover licenses and hosting at the discretion of

EPCH.

- Fees charged by the vendor for customized work at the request of a Participating Organization will be passed through to the organization unless alternate arrangements are made directly with the EPCH Executive Director.
- Any fees charged must be remitted within 60 days of the date on the related invoice unless alternate arrangements are made directly with the EPCH Executive Director.

2.9 Computer Equipment and Supplies

Policy:

EPCH HMIS may provide computer equipment and supplies to the HMIS Users.

Procedure:

Consult EPCH HMIS Lead Agency regarding computer equipment and supplies availability and policies.

3. SECURITY POLICIES AND PROCEDURES

3.1 User Authentication

Policy:

EPCH HMIS can only be accessed with a valid username and password combination. The HMIS Administrator will provide unique username and initial password for eligible individuals after completion of required training which includes a review of these Policies & Procedures.

Procedure:

- The Participating Organization will determine which of their employees will have access to the EPCH HMIS. User access will be granted only to those individuals whose job functions require legitimate access to the system.
- Proposed User must complete the required training and demonstrate proficiency in use of system.
- Proposed User must sign the HMIS User Agreement upon initial access to the system, stating that he will abide by the Policies & Procedures, will appropriately maintain the confidentiality of client data, and will only collect, enter and retrieve data in the system relevant to the delivery of services to people.
- The HMIS Administrator will assign new user with a username and an initial password.
- Sharing of usernames and passwords will be considered a breach of the HMIS User Agreement as it compromises the security to clients.
- Organization Administrator is required to notify the HMIS Administrator immediately when a User leaves employment with the organization or no longer needs access.
- HMIS Administrator will terminate access upon written notification (email is acceptable) by the Organization Administrator, Executive Director (or other empowered officer) within 24 hours.

3.2 Passwords

Policy:

User will have access to the EPCH HMIS via a username and password. User will maintain passwords confidential.

Procedure:

- The HMIS Administrator will provide new User a unique username and temporary password after required training is completed.
- User will be required to create a permanent password that is between eight and sixteen characters in length. It must also contain characters from the following four categories: (1) uppercase characters (A through Z), (2) lower case characters (a through z), (3) numbers (0 through 9), and (4) non-alphabetic characters (for example, \$, #, %).
- After 30 minutes of inactivity, User will get a session timeout warning popup that will allow Users to continue their session or will automatically log the user off after 30 minutes of inactivity.
- Access permission will be revoked after the User unsuccessfully attempts to log on three (3) times. The User will be unable to gain access until they have contacted the HMIS Help Desk to reset their password.

3.3 Extracted Data

Policy:

Users will maintain the security of any client data extracted from the EPCH HMIS and stored locally, including all data contained in custom reports. Users may not electronically transmit unencrypted client data across a public network.

Procedure:

- Data extracted from the EPCH HMIS and stored locally will be stored in a secure location and will not be transmitted outside of the private local area network unless it is properly protected.
- Personal identifiable client data will not be distributed through email.
- Any security questions can be addressed to the HMIS Administrator.

3.4 Hardware Security Measures

Policy:

All computers and networks used to access EPCH HMIS must have virus protection software and firewall installed. Virus definitions and firewall must be regularly updated.

Procedure:

- HMIS Lead Agency must confirm that Participating Organizations has virus protection software and firewall installed prior to granting EPCH HMIS access.
- Virus definition must be updated regularly.

- Firewall must be placed between any computer and internet connection for the entire network, be protected with at minimum Wired Equivalent Privacy (WEP), use Network Address Translation (NAT), and maintain the most recent virus security updates.

3.5 Backup and Recovery Procedures

Policy:

The El Paso HMIS employs information security and risk prevention practices that meet or exceed the minimum standards required by HUD, the State of Texas, and the City of El Paso. All client-level data in the El Paso HMIS is hosted in secure, US-based facilities regularly evaluated for security and privacy best practices. At a minimum, data center facilities maintain current, independent audits certifying compliance with industry standards:

Procedure:

- The vendor's most recently updated [Disaster Recovery Plan](#) is embedded in these Policies & Procedures and available for review.
- The vendor's most recently updated [Information Security](#) summary is embedded in these Policies & Procedures and available for review.
- The vendor will provide El Paso with copies of these audits upon request.

3.6 Security Review

Policy:

EPCH HMIS Lead Agency will complete an annual security review to ensure the implementation of the security requirements for itself and Participating Organizations.

Procedure:

- EPCH HMIS Agency will conduct a security review that includes the completion of a security checklist ensuring that each security standard is implemented.

3.7 Security Violations and Sanctions

Policy:

Any User found to be in violation of security protocols of the organization procedures or Policies and Procedures will be sanctioned accordingly. All Users must report potential violations of any security protocols described in the Policies and Procedures.

Procedure:

- Users are obligated to report suspected instances of noncompliance and/or security violations to the Organization Administrator or HMIS Administrator as soon as possible.
- The Organization Administrator or HMIS Administrator will investigate potential violations.
- Any User found to be in violation of security protocols will be sanctioned accordingly. Sanction may include but are not limited to suspension of system

privileges and revocation of system privileges.

4. OPERATIONAL POLICIES AND PROCEDURES

4.1 User Access Levels

Policy:

All User will be designated a user access level that controls the level and type of access the user has to data and functionality within the EPCH HMIS.

Procedure:

- HMIS Administrator, in consultation with the Participating Organization, will assign the level and type of access the user will have in the system.
- HMIS Administrator will terminate access within three (3) days upon written notification from the Organization Administrator, Executive Director or other empowered officer.
- HMIS Administrator will revoke user access to anyone suspected or found to be in violation of the policies outlined in this document or the HMIS User Agreement.

4.2 Training

Policy:

Each User must complete the required training and any additional training relevant to their position prior to gaining access to the EPCH HMIS. HMIS Administrators will provide training to all Users.

Procedure:

- HMIS Administrator will provide Basic User Training to proposed Users.
- User must successfully complete the Basic User Training to demonstrate proficiency in the system and understanding of the Policies & Procedures.
- HMIS Administrator will provide a review of the Policies & Procedures.
- Users are encouraged to attend monthly HMIS Steering Committee meetings as part of the ongoing training initiative of the HMIS Administrator (see Item 1.5 regarding Participating Organization attendance requirement.)

4.3 Client Consent to Share Information and Confidentiality

Policy:

Participating Organizations must obtain informed, signed consent prior to either entering or accessing any client protected personal information (PPI) into the EPCH HMIS. Services will not be denied if client chooses not to include personal information. Personal information collected about the client should be protected. Each Participating Organization and User must abide by the terms in the HMIS Participating Organizations Agreement and HMIS User Agreement.

Procedure:

- Client must sign Consent to Share Protected Personal Information (Appendix C).
- Clients that provide permission to enter personal information allow for Participating Organizations within the region to share client and household demographic data.
- Participating Organizations must store signed Consent to Share Protected Personal Information Agreement in client record for auditing purposes.
- Participating Organizations must post a Notice Regarding Collection of Personal Information (Appendix E) that explains the uses and disclosures of information.
- Participating Organizations must provide a copy of the Privacy Notice upon request.
- If a client refuses to provide consent, the User should not include any personal identifiers (such as first name, last name, social security number, date of birth, etc.) in the client record. Instead, User should include a client identifier to recognize the record in the system.
- Participating Organizations shall comply with Federal and State confidentiality laws and regulations that protect client records.

HIPAA-Covered Entities:

An organization that is covered under the HIPAA standards is not required to comply with the HMIS privacy or security standards, so long as the organization determines that a substantial portion of its protected information about homeless clients or homeless individuals is indeed protected health information as defined in the HIPAA rules.

HIPAA standards take precedence over HMIS because HIPAA standards are finely attuned to the requirements of the health care system; they provide important privacy and security protections for protected health information; and it would be an unreasonable burden for providers to comply with and/or reconcile both the HIPAA and HMIS rules. This spares organizations from having to deal with the conflicts between the two sets of rules.

4.4 Revocation of Consent

Policy:

In the event that a client previously gave consent to share their PPI in the EPCH HMIS and chooses at a later date to revoke consent, a Revocation of Consent (Appendix G) must be signed by client.

Procedure:

- Upon request, the Participating Organization must modify the client information by removing any personal identifiers (First Name, Last Name, Social Security Number, and Date of Birth) from the client record.
- Users should include a client identifier to recognize the record in the system.
- Participating Organization's that have previously provided services will still have access to client protected personal information.

4.5 Data Sharing

Policy:

Last updated on: 11/18/2020

Client data (with consent) contained in EPCH HMIS will be shared with other Participating Organizations.

Procedure:

- Data sharing refers to the sharing of information between Participating Organizations for the coordination of case management and client service delivery.
- Users found to be sharing program level client data without consent will have their access terminated.

4.6 Client Record Access

Policy:

Client may obtain and inspect a copy of their client information. The Participating Organization, as the custodian of the client data, has the responsibility to provide the client with the requested information except where exempted by state and federal law.

Procedure:

- Client information contained in the universal data elements can be provided at any organization the client requests it from, if the client has previously given the other organization consent to share and that consent is still in force. The Participating Organization may not share any client information entered by other agencies beyond the universal data elements.
- The Organization Administrator or User will review client information with client if he or she requests to view their HMIS data.
- No client shall have access to another client record in the system.
- A copy of the requested data will be provided to client within a reasonable time frame.
- Parental or guardian access will be decided based upon existing organization guidelines.

4.7 Client Grievance

Policy:

Clients will file grievances with Participating Organizations. Participating Organizations must have written grievance procedures that can be provided to client upon request. Any unresolved grievances may be escalated to the EPCH HMIS Lead Agency.

Procedure:

- Clients will submit grievance directly to Participating Organizations with which they have a grievance.
- Upon client request, Participating Organizations will provide a copy of their grievance procedure and the EPCH HMIS Policies & Procedures.
- The Participating Organization will be responsible to answer any questions and complaints regarding the EPCH HMIS. A record of all grievance and any attempts made to resolve the issue must be kept in file. If the grievance is resolved, Participating Organizations will include the date and a brief description of the resolution. For any written complaint, Participating Organizations must send a copy

to the EPCH HMIS Lead Agency.

- If the Participating Organization is unable to resolve the problem, the client must complete the Grievance Form (Appendix G) outlining the date of incident, name of parties involved, description of the incident, and their contact information for follow-up. Participating Organizations must forward a copy of the completed Grievance Form to the EPCH HMIS Lead Agency.
- The EPCH HMIS Lead Agency will review and determine the need for further action.

5. DATA POLICIES AND PROCEDURES

5.1 Data Quality Management Plan

Policy:

All data entered into the EPCH HMIS must meet data quality standards. Users will be responsible for the quality of their data entry. While focusing on data quality for federally-funded projects that enter data into HMIS is necessary to ensure accurate reporting for those grants, any project that enters data into HMIS contributes to the overall picture of homelessness within the CoC, and therefore, is expected to participate in this Data Quality Management Plan.

- **Definition:** Data Quality is a term that refers to the reliability and validity of client-level in the HMIS. It is measured by the extent to which data in the system reflects actual information in the real world. With good data quality a CoC can accurately tell its story of the individuals and families it serves. Data Quality Benchmarks to be evaluated by recommendation of HUD include (1) Timeliness, (2) Completeness, (3) Accuracy, (4) User Access and Consistency and (5) Bed Coverage.
- The reasons why Data Quality is important are many, including but not limited to:
 - Requirements based on funding the CoC receives;
 - Data Quality, or lack thereof, can directly affect the funding opportunities for providers;
 - Accurate reporting for federal, state, and local funding;
 - The ability of the CoC, and providers within the CoC, to tell the story of homelessness as realistically and completely as possible; and
 - The data entered into HMIS directly affects clients through the Coordinated Entry process and may determine which services they may or may not be eligible for.

Procedure:

- Participating Organizations must sign the HMIS Participating Organization Agreement to ensure that all participating projects are aware and have agreed to the Data Quality standards.
- Upon agreement, Participating Organizations will collect and enter as much relevant client data as possible for the purposes of providing services to that client based on the data elements described under item 2.3 and in conformance with the most recently approved HUD HMIS Data Standards Manual.
- All data will be input into the system as described under the Timeliness Data Quality

Standard below.

- The HMIS Administrator will conduct regular checks for Data Quality and User access. Any patterns of errors or missing data will be reported to the Organization Administrator or User as described in the Data Quality category below.
- Users will be required to correct the identified data errors and will be monitored for compliance by the Organization Administrator and/or the HMIS Administrator.
- Users may be required to attend additional training as needed.
- Providers or Users may be locked out of HMIS until they receive refresher or additional training from the HMIS Lead and show that Data Quality is a focus.
- User access may be denied if Data Quality becomes a consistent issue that is not acknowledged or addressed.
- Agencies may be prevented from applying for new or additional dollars during RFP processes if Data Quality continues to be an issue.
- EPCH as HMIS Administrator and CoC Lead will work to ensure Users have access to all the support and tools they need to ensure a high level of Data Quality within the HMIS.
- EPCH will monitor Data Quality, present Data Quality issues and concerns to the CoC Board four (4) times a year, annually acknowledge the work of providers meeting a high level of Data Quality, use Data Quality during the rating and ranking process for CoC Program funding and will work with state and local funders to also use Data Quality metrics when making funding allocation decisions to providers.

Data Timeliness:

Users must enter all universal data elements and program-specific data elements within four (4) days of collection of a client entering or exiting a program. Data Timeliness reports will be generated on a quarterly basis and sent to providers. Those providers who do not meet this standard will be asked to work with the HMIS Administrator to make sure that they can meet the Data Timeliness standard moving forward. For consistent issues with Data Timeliness, providers may be directed to create a Data Quality Improvement Plan (DQIP).

Data Completeness:

All data entered into the system must be complete, unless otherwise authorized by the HMIS Administrator, following data collection standards set by the HUD HMIS Data Standards currently in place. Data Completeness reports will be generated monthly and sent to providers. Those providers who fail to meet the requirement for Data Completeness will be asked to clean up their data within five (5) working days. For consistent issues with Data Completeness, providers may be directed to create a DQIP.

Data Accuracy:

All data entered shall be collected and entered in a common and consistent manner across all programs. Data Accuracy is not as easy to manage or monitor and requires agencies to verify information provided to them monthly on the HMIS Attendance report. The HMIS Lead will run reports on a monthly basis and send to providers. The goal for all project types and all data entered into HMIS is 100% Data Accuracy. Data accuracy is expected to be addressed within two (2) weeks of receipt of the

Attendance Report. Additional data elements will be reviewed by the HMIS Administrator including but not limited to:

- Date of birth and project start date (ensure the two are not the same, especially for Heads of households);
- 3.917 data elements (ensure that the responses to residence prior to project entry, length of time in previous place, approximate date homelessness started, number of times experiencing homelessness in the last three years, and number of months experiencing homelessness in the last three years do not conflict with each other);
- Disabling Condition yes / no and types of disabling conditions (ensure these do not conflict);
- Health Insurance yes / no and sources of insurance (ensure these do not conflict);
- Income yes / no and sources of income (ensure these do not conflict);
- Non-Cash Benefits yes / no and sources of non-cash benefits (ensure these do not conflict);
- Domestic violence victim / survivor and subsequent data elements (if the first answer is no, are the other questions answered, and vice versa);
- Relationship to head of household (are there multiple heads of household or no head of household?);
- Client location (is the client location defined as a community outside of the applicable CoC?);
- Veteran (is a minor-aged individual defined as a veteran?);
- A given project only includes clients of a specific gender (if that project is not dedicated to only serving a specific gender)

The Longitudinal System Analysis looks at specific data quality issues in relation to that system-wide submission to HUD on an annual basis. These specific data quality and data accuracy pieces will be addressed in the reports run by the HMIS Administrator on an ongoing basis. The CoC will also work with providers to review, at regular intervals, the data collected directly from clients, either on paper forms or by being present during intakes with clients, and the data entered into HMIS to ensure that the data entered into HMIS matches the client's reality. This will be done, at a minimum, during annual formal onsite monitoring visits, and will also occur at other points throughout the year. Those providers who show issues with Data Accuracy will be asked to clean up their data within a certain timeframe. For consistent issues with Data Accuracy, providers may be directed to create a DQIP.

User Access and Consistency: Users with access to HMIS should be entering data on a regular and consistent basis, not only to prevent a backlog of data entry, but also to ensure Users maintain familiarity with the HMIS and the workflows for which they are responsible.

The HMIS Lead will monitor User log in and access to HMIS monthly by running a report that shows when Users last logged into the system. If Users have not logged into HMIS within the last 30 days of the report run date, the HMIS Administrator will contact the User and ask if they still need access to the system. If the User responds that they do still need access, the HMIS Administrator will ensure that the User has maintained sufficient Data Quality and does not need refresher training. If the user does not have a high level of data quality, refresher training will be recommended.

If the User is non-responsive to any inquiries about their access to HMIS, the HMIS Administrator (or EPCH Planning staff) will contact the User's direct supervisor to recommend the refresher training. Should the HMIS not hear from either the User or the User's direct supervisor, the user license will be removed from the system.

Bed Coverage: The importance of a high percentage of HMIS Bed Coverage for all project types is an emphasis of the [HUD TA Data Strategy](#). Without a high percentage of HMIS Bed Coverage within a CoC, the data within HMIS is never holistic and the story told with HMIS data about homelessness within the CoC is never fully accurate. A lack of high HMIS Bed Coverage prevents CoCs from truly understanding how both their system, and the clients served within their system, are functioning. Therefore, the goal for HMIS Bed Coverage for all project types is 100%.

EPCH will ensure that bed coverage is as close to 100% as is possible for all project types. This includes a review of the CoC's most recent Housing Inventory Chart (HIC) to know which providers participated in the most recent HIC but are not entering data into HMIS and including any new projects that become available to serve clients at-risk of or experiencing homelessness. EPCH will take the following steps to ensure HMIS Bed Coverage reaches or maintains at 100%:

- Review the HIC on a semi-annual basis to ensure all projects (with the exception of Victim Services Providers) are entering data into HMIS;
- If projects are included on the most recent HIC that do not enter data into HMIS, EPCH should find out why this is the case and target any solutions to the specific "why";
- For any new project that becomes available within the CoC that will serve clients at-risk of or experiencing homelessness, EPCH should be made aware and work to ensure the new project is encouraged and / or required to enter data into HMIS.

5.2 Data Use and Disclosure

Policy:

All Users will follow the data use Policies and Procedures to guide the data use of client information stored in the EPCH HMIS.

Definitions:

Client data may be used or disclosed for system administration, technical support, program compliance, analytical use, and other purposes as required by law, and as outlined by the Privacy Notice, HMIS Participating Organization Agreement and HMIS User Agreement. Uses involve sharing parts of client information with persons within an organization. Disclosures involve sharing parts of client information with persons or organizations outside an organization.

Procedure:

- Participating Organizations may use and disclose data contained in the system to support the delivery of services to clients experiencing homelessness or at-risk of homelessness in El Paso County/City.
- Each organization shall have access to their respective agencies' client data

stored in the system. The CoC will use the data for various purposes including; administrative functions, technical support, program compliance, and analytical use. Unless restricted by other laws, the information collected can be shared and disclosed under the circumstances outlined in the Privacy Notice. Upon signing the client consent form, protected personal information may be disclosed for service provision purposes.

- The vendor and any authorized subcontractor shall not use or disclose data stored in HMIS without expressed written permission in order to enforce information security protocols. If granted permission, the data will only be used in the context of interpreting data for research and system troubleshooting purposes. The Service and License Agreement signed individually by the HMIS Lead and vendor contain language that prohibits access to the data stored in the software except under the conditions noted above.

5.3 Data Release

Policy:

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

Definition:

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

Procedure:

- No identifiable client data will be released by Participating Organizations to any person, agency, or organization for any purpose without written permission from the client.
- The organization may not release personal identifiable client data without written permission from the client. Organizations may release program and/or aggregate level or de-identified data for all clients to whom the organization provided services.
- EPCH HMIS may release aggregate or de-identified data about the continuum at the program, sub-regional, and regional level. Aggregate or de-identified data may be released without organization permission at the discretion of the Continuum. CoC Board.
- The EPCH CoC may develop an annual release of aggregate data in a summary report format.

5.4 Data Migration

Policy:

Data migration or uploads from legacy systems is not allowed, unless approved by the HMIS Administrators.

Definition:

Data migration (or conversion): a one-time process of transferring data from any existing system to the EPCH HMIS. Upon transfer, the organization abandons its existing system and uses the EPCH HMIS for recording all client-related data.

Data uploads (transfers): ongoing, periodic process of transferring data from an existing system to the EPCH HMIS. Data uploads follow the same procedures as above, but the organization continues to use its existing system for recording all client-related data.

Procedure:

- Migrated data must be non-duplicated and an exact match to the existing field type of the EPCH HMIS. The Participating Organizations will be responsible for the accuracy, completeness, and quality of the migrated data.
- Only data that is matched using agreed upon methods with EPCH HMIS data fields may be migrated. Data must be unduplicated prior to data migration. All required fields in the EPCH HMIS are required for migration. A data dictionary will be provided upon request.
- The HMIS Administrator will decide the appropriate data migration candidates. If approved, a Memorandum of Understanding or other agreement must be completed and the Organization will provide current data in the agreed upon format to the HMIS Administrator.
- If the data cannot be migrated, manual conversion (data entry by the organization's personnel) may be necessary to move data from legacy systems into the EPCH HMIS.
- Unless negotiated prior to migration/upload, the organization choosing to migrate or upload data will bear all costs associated with these processes.

6. TERMINOLOGY

Aggregate Data: Data with identifying elements removed and concentrated at a central server. Aggregate data are used for analytical purposes and reporting.

Anti-Virus Software: Programs to detect and remove computer viruses. The anti-virus software should always include a regular update services allowing it to keep up with the latest viruses as they are released.

Audit Trail: A history of all access to the system, including viewing, additions and updates made to a client record.

Authentication: The process of identifying a user in order to grant access to a system or resource usually based on a username and password.

BitFocus Inc: Software developer of the Clarity Human Services for the EPCH HMIS.

Client: The person receiving services whose information is entered into the EPCH HMIS.

Continuum of Care (CoC): Refers to the range of services (outreach, emergency transitional and permanent housing and supportive services) available to assist people out of homelessness.

Data Quality Improvement Plan (DQIP): Refers to a documented plan to improve Data Quality using improvement strategies recommended by EPCH.

Database: An electronic system for organizing data so it can easily be searched and retrieved. The data within the EPCH HMIS is accessible through the web-based interface.

Decryption: Conversion of scrambled text back into understandable, plain text form. Decryption uses an algorithm that reverses the process used during encryption.

EPCH HMIS: The El Paso Coalition for the Homeless Management Information System provided by the vendor and tailored for use in El Paso City & County region.

EPCH HMIS Steering Committee: Comprised of at least one representative from each of the EPCH Participating Agencies. Convenes monthly to discuss system issues, receive updates, training and provide feedback.

Encryption: Conversion of plain text into encrypted data by scrambling it using a code that masks the meaning of the data to any unauthorized viewer. Encrypted data are not readable unless they are converted back into plain text via decryption.

Firewall: A method of controlling access to a private network, to provide security of data. Firewalls can use software, hardware, or a combination of both to control access.

HMIS: Homeless Management Information System. Refers to the geographic system used by a CoC to manage data about the use of homeless services.

HMIS Administrator: The person(s) with the highest level of user access in each CoC. This user has full access to all user and administrative functions in the CoC and will serve as the liaison between Participating Organizations and the vendor.

HMIS User: An individual who has unique user identification and directly accesses the EPCH HMIS to assist in data collection, reporting or administration as part of their job function in homeless service delivery.

Local Area Network (LAN): A network that is geographically limited, allowing easy interconnection of computers within offices or buildings.

Network: Several computers connected to each other.

Organization Administrator: The person responsible for system administration at the organization level. Responsibilities include informing HMIS System Administration of the need to add and delete Users, basic trouble-shooting, and escalation of issues to their HMIS Administrator.

Participating Organizations: An organization that operates a project that either contributes data to an HMIS or has direct access to PPI in HMIS.

Server: A computer that provides a service for other computers connected to it via a network. Servers can host and send files, data or programs to client computers.

User ID: The unique identifier assigned to an authorized HMIS User.

7. APPENDICES

Appendix	Document Title
Appendix A	HMIS Participating Organization Agreement
Appendix B	HMIS User Agreement
Appendix C	Consent to Share Protected Personal Information
Appendix D	Privacy Notice
Appendix E	Note Regarding Collection of Personal Information
Appendix F	Revocation of Consent
Appendix G	Grievance Form
Appendix H	Client Rights Brochure

Appendix A: HMIS Participating Organizations Agreement

El Paso Coalition for the Homeless
Homeless Management Information System (HMIS)
PARTICIPATING ORGANIZATIONS AGREEMENT

I. Purpose

The HMIS is the secured electronic database for the El Paso CoC and is a valuable resource. The goal is to provide a comprehensive case management system to advance the provision of quality services for homeless persons, improve data collection, and promote more responsive policies to end homelessness.

II. Agreement and Understanding

This Agreement authorizes your organization's HMIS User(s), to enter Protected Personal Information (PPI) into HMIS, as authorized by your organization and the El Paso Coalition for the Homeless HMIS Administrator. Your HMIS User(s) must complete the necessary training(s) prior to receiving a unique HMIS User Identification (User ID) and password.

III. Confidentiality and Informed Consent

Confidentiality: User(s) must abide by its organization's policies and procedures; uphold all privacy protection standards; and comply with all relevant federal and State confidentiality laws and regulations that protect client records.

Written Consent: To obtain written consent, prior to each client's assessment, Users must inform each client that the client's information will be entered into an electronic database called HMIS. Users must also explain the terms of the Consent to Share Protected Personal Information form. Each client who agrees to have his or her PPI entered into HMIS must sign the Consent to Share Protected Personal Information form.

Verbal Consent: Verbal consent to enter PPI into HMIS may be obtained during circumstances such as phone screenings, street outreach, or community access center sign-ins. Users must inform each client that the client's information will be entered into the HMIS database. Users must also explain the terms of the *Consent to Share Protected Personal Information* form. The client's written consent must be obtained once the client appears for his or her initial assessment.

IV. Client's Rights

- A client may not be denied services for failure to provide consent for HMIS data collection.
- A client has the right to inspect, copy, and request changes in their HMIS records.
- A client's consent may be revoked by that client at any time through a written notice or by completing the *Revocation of Consent form*.
- A copy of the Privacy Notice must be provided at the time the client requests.
- Each client has the right to receive the following, no later than five (5) business days of a written request:
 - A correction of inaccurate or incomplete PPI
 - A copy of his or her consent form;
 - A copy of his or her HMIS records; and

- A current list of Participating Organizations that have access to HMIS data

Right to Make Corrections

If the client believes that their PPI in HMIS is incorrect or incomplete, the client has the right to request for a correction. To ask for either of these changes, the client will need to send a written request, including the reason why he or she believes the information is incorrect or incomplete to the HMIS Administrator of the organization that entered the information into HMIS. The organization may turn down the request if the information:

- Was not created by the organization you are requesting the change from;
- Is not part of the information that you would be allowed to look at and copy;
- Is related to another individual;
- Is found to be correct and complete;
- Is otherwise protected by law.

However, if your request for correction is denied, you have the right to request that the following language is entered next to a particular entry: “The participant disputes the accuracy of this entry.”

V. Data Use

This Organization must protect HMIS data by ensuring that:

- A link to the Privacy Notice is accessed from Organization’s website.
- EPCH HMIS is not accessible to unauthorized Users
- EPCH HMIS is only accessed by computers approved by the Organization
- EPCH HMIS Users are trained regarding user responsibilities and conduct
- EPCH HMIS Users who violate the User Agreement are reported to the HMIS Administrator within 24 hours of knowledge of the violation, including violations that are not directly related to the use of HMIS.
- HMIS Users sign and comply with the EPCH *HMIS User Agreement*

VI. Responsibilities

This Organization is responsible to ensure that:

- The *Notice Regarding Collection of Personal Information* is posted at each intake desk or comparable location.
- HMIS Users do not misuse the system
- Clients are notified if a breach of their PPI is discovered
- Any HMIS User who finds a possible security lapse on the system is obligated to immediately report it to the HMIS Administrator.
- A signed copy of the *Consent to Share Protected Personal Information* is retained for a period of seven (7) years after the PPI was created or last changed.
- HMIS standards are adhered to as described in the HMIS Policies & Procedures for:
 - Completion of the HMIS Participating Organizations Agreement.
 - Attendance at a minimum of 75% of monthly HMIS Steering Committee meetings within a 12-month period.
 - Compliance with Data Quality standards.
 - Financial requirements.
 - New organization set-up within two (2) months.

VII. System Use

Computer equipment and services provided by the CoC are intended only for HMIS-related activities.

Prohibited uses include, but are not limited to: malicious or illegal activities; unauthorized access; the creation, sending and/or storing of fraudulent, threatening, harassing, or obscene messages; inappropriate mass mailing (spamming, flooding, bombing); denial of service attacks; and the creation or intentional distribution of computer viruses, worms, and/or Trojan horses.

Equipment, if applicable: All CoC-provided computer equipment including, but not limited to, printers, scanners, laptops and monitors, were provided through grant funds from HUD. The maintenance and upgrades of these devices are subject to the requirements and funding limitations of the HUD grant. Maintenance and/or upgrade costs to equipment, incurred after the HUD grant funds have been exhausted, become the sole responsibility of this Organization.

Software, Licenses, and/or Services, if applicable: CoC-provided services to each organization may include, but are not limited to, purchasing and installing Anti-Virus Software and licenses, Firewall software and licenses, Windows software updates and High-Speed Internet Connections. The software and/or services are provided for HMIS purposes through HUD grant funds. The maintenance, upgrades and license purchases are subject to the requirements and funding limitations of the HUD grant. Additional maintenance, upgrades and license purchases, incurred after the grant funds have been exhausted, become the sole responsibility of this Organization.

VIII. Rights and Privileges

EPCH HMIS data is stored in one central database and is owned by the EPCH HMIS. The EPCH HMIS reserves all rights to the HMIS data. Use of the EPCH HMIS equipment, software, licenses, and/or services is a privilege and is assigned and managed by the HMIS Lead, EPCH.

IX. Copyright

The EPCH HMIS and other CoC-provided software are protected by copyright and are not to be copied, except as permitted by law or by contract with the owner of the copyright. The number and distribution of copies of any CoC-provided software are at the sole discretion of the HMIS Lead, EPCH.

X. Violations

Any violations or suspected violations of any of the terms and conditions of this agreement, the HMIS User Agreement, and/or the HMIS Policies and Procedures, must be immediately and confidentially reported to the HMIS Administrator and the Executive Director or other authorized representative of this Organization.

XI. Term

This Participating Organizations Agreement becomes effective on the date of final execution and shall remain in effect unless terminated pursuant to paragraph XI. Termination, below.

XII. Amendment and Termination

- The EPCH CoC reserves the right to amend this agreement by providing a 3-day notice to this Organization.
- Either party has the right to terminate this agreement, with or without cause, by providing a 3-day written notice to the other party.

- If this agreement is terminated, this Organization shall no longer have access to HMIS or any information therein. The remaining HMIS Participating Organizations shall retain the right to use all client data previously entered by this Organization, subject to any restrictions requested by the client.

All organizations that sign this agreement and are granted access to the EPCH HMIS agree to abide by EPCH's HMIS Policies and Procedures. The signature of the Executive Director or other authorized representative of this Organization indicates acceptance of all terms and conditions set forth in this agreement.

This Agreement is executed between the EPCH and the Participating Organizations. Upon final execution, this Organization will be given access to the EPCH HMIS.

Organization Name	EPCH Name
-------------------	-----------

Organization Administrator/Authorized Representative (Print Name)	HMIS Administrator Name (Print Name)
--	---

Signature	Signature
-----------	-----------

Date of Signature	Date of Signature
-------------------	-------------------

B: HMIS User Agreement

EPCH

HOMELESS MANAGEMENT INFORMATION SYSTEM (HMIS) USER AGREEMENT

I. Purpose

The EPCH HMIS is the secured electronic database for the El Paso City/ County CoC and is a valuable resource. The EPCH's HMIS goal is to provide a comprehensive case management system to advance the provision of quality services for homeless persons, improve data collection, and promote more responsive policies to end homelessness in the El Paso County/City.

II. Agreement and Understanding

This Agreement authorizes you, an HMIS User (User), to enter Protected Personal Information (PPI) into the EPCH HMIS, as authorized by your organization and the CoC HMIS Administrator. You must complete the necessary training(s) prior to receiving a unique HMIS User Identification (User ID) and password.

II. Client Confidentiality and Informed Consent

Confidentiality: This User must abide by its organization's policies and procedures; uphold all privacy protection standards established by the EPCH HMIS Policies and Procedures; and comply with all relevant federal and State of Texas confidentiality laws and regulations that protect client records.

Written Consent: To obtain written consent, prior to each client's assessment, Users must inform each client that the client's information will be entered into an electronic database called HMIS. Users must also explain the terms of the *Consent to Share Protected Personal Information* form. Each client who agrees to have his or her PPI entered into the EPCH HMIS must sign the *Consent to Share Protected Personal Information* form.

Verbal Consent: Verbal consent to enter PPI into the EPCH HMIS may be obtained during circumstances such as phone screenings, street outreach, or community access center sign-ins. Users must inform each client that the client's information will be entered into the HMIS database. Users must also explain the terms of the *Consent to Share Protected Personal Information* form. The client's written consent must be obtained once the client appears for his or her initial assessment.

III. Client Rights

- A client may not be denied services for failure to provide consent for EPCH HMIS data collection.
- A client has the right to inspect, copy, and request changes in their EPCH HMIS records.
- A client's consent may be revoked by that client at any time through a written notice or by completing the Revocation of Consent form.
- A copy of the Privacy Notice must be provided at the time the client requests.

- Each client has the right to receive the following, no later than five (5) business days of a written request:
 - A correction of inaccurate or incomplete PPI
 - A copy of his or her consent form;
 - A copy of his or her HMIS records; and
 - A current list of Participating Organizations that have access to HMIS data.

Right to Make Corrections

If the client believes that their PPI in HMIS is incorrect or incomplete, the client has the right to request for a correction. To ask for either of these changes, the client will need to send a written request, including the reason why he or she believes the information is incorrect or incomplete to the HMIS Administrator of the organization that entered the information into HMIS. The organization may turn down the request if the information:

- Was not created by the organization you are requesting the change from;
- Is not part of the information that you would be allowed to look at and copy;
- Is related to another individual;
- Is found to be correct and complete;
- Is otherwise protected by law.

However, if your request for correction is denied, you have the right to request that the following language is entered next to a particular entry: “The participant disputes the accuracy of this entry.”

IV. User Responsibilities and Conduct

I understand and agree that:

- I have an ethical and a legal obligation to ensure that the data I collect and enter into HMIS is accurate and does not misrepresent the client’s information.
- I will not reveal or release PPI to unauthorized organizations, individuals or entities.
- I will use the data within the HMIS only for the purposes of homeless service delivery.
- I am not permitted to access the HMIS from any computer that has not been designated or approved by my organization.
- I will never use the HMIS to perform an illegal or malicious act.
- I acknowledge that HMIS contains confidential and sensitive information. Accordingly, I understand and agree that my access to HMIS may be suspended and/or permanently revoked as a result of my unethical or illegal actions, even if those actions were not related to my use of HMIS. Unethical or illegal actions may include, but are not limited to, breach of trust or fiduciary duty, harassment, fraud, threats, etc., in relation to person seeking or receiving services.
- I authorize this Organization to release any and all information, related to my unethical or illegal conduct mentioned above, to the HMIS Administrator
- I will not attempt to increase the level of access to which I am authorized, or attempt to deprive other HMIS Users of access to the HMIS.
- My HMIS User ID and password shall be kept secure and will not be shared.
- I will refrain from leaving my computer unattended while logged into the system.
- I will protect and store client information printed from HMIS in a secure location.

- I will dispose of PPI printed from HMIS, when it is no longer needed, in a manner that maintains client confidentiality.
- If I suspect or encounter a security breach, I will immediately notify my organization’s HMIS administrator.
- If my relationship with my organization changes or terminates, any client information that I entered into or obtained from the HMIS must remain confidential.
- Discriminatory comments based on race, color, religion, national origin, ancestry, handicap, age, sex and sexual orientation are not permitted in the HMIS. Profanity and offensive language are also not permitted in the HMIS.
- PPI that is transmitted electronically must be password protected to maintain confidentiality.
- I will comply with my organization’s policies and procedures and the EPCH HMIS Policies and Procedures in my use of HMIS. The EPCH HMIS Policies and Procedures can be accessed from in the EPCH website.
- If the HMIS Administrator updates or makes changes to this Agreement, I will be provided with a written notice of the changes from the Organization named below. I understand and agree that I will be responsible to comply with all such updates and/or changes.
- Any violation of this User Agreement is grounds for immediate suspension or revocation of my access to the HMIS.

My signature below confirms my agreement to comply with all the provisions of this EPCH HMIS User Agreement.

Organization Name

Organization Administrator/Authorized Representative
(Print Name)

User First and Last Name (Print Name)

Signature

Signature

Date of Signature

Date of Signature

Appendix C: Consent to Share Protected Personal Information

EPCH

HOMELESS MANAGEMENT INFORMATION SYSTEM (HMIS) CONSENT TO SHARE PROTECTED PERSONAL INFORMATION

The EPCH HMIS is a local electronic database that securely record information (data) about clients accessing housing and homeless services within the El Paso County/City geographic area. This organization participates in the HMIS database and shares information with other organizations that use this database. This information is utilized to provide supportive services to you and your household members.

What information is shared in the HMIS database?

We share both Protected Personal Information (PPI) and general information obtained during your intake and assessment, which may include but is not limited to:

- Your name and your contact information
- Your social security number
- Your birthdate
- Your basic demographic information such as gender and race/ethnicity
- Your history of homelessness and housing (including your current housing status, and where and when you have accessed services)
- Your self-reported medical history, including any mental health and substance abuse issues
- Your income sources and amounts; and non-cash benefits
- Your veteran status
- Your disability status
- Your household composition
- Your photo (optional)

How do you benefit from providing your information?

The information you provide for the HMIS database helps us coordinate the most effective services for you and your household members. By sharing your information, you may be able to avoid being screened more than once, get faster services, and minimize how many times you tell your 'story.' Collecting this information also gives us a better understanding of homelessness and the effectiveness of services in your area.

Who can have access to your information?

Organizations that participate in the HMIS database can have access to your data. These organizations may include homeless service providers, housing groups, healthcare providers, and other appropriate service providers.

How is your personal information protected?

Your information is protected by the federal HMIS Privacy Standards and is secured by passwords and encryption technology. In addition, each Participating Organizations has signed an agreement to maintain the security and confidentiality of the information. In some instances, when the Participating Organizations is a health care organization, your information may be protected by the privacy

standards of the Health Insurance Portability and Accountability Act (HIPAA).

By signing below, you understand and agree that:

- You have the right to receive services, even if you do not sign this consent form.
- You have the right to receive a copy of this consent form.
- Your consent permits any participating organization to add to or update your information in HMIS, without asking you to sign another consent form.
- This consent is valid for seven (7) years from the date the PPI was created or last changed.
- You may revoke your consent at any time, but your revocation must be provided either in writing or by completing the *Revocation of Consent* form. Each Participating Organization that entered information into HMIS will continue to have access to your PPI, but the information will no longer be available to any other Participating Organization.
- The Privacy Notice for the EPCH HMIS contains more detailed information about how your information may be used and disclosed. A copy of this notice is available upon request.
- No later than five (5) business days of your written request, we will provide you with:
 - A correction of inaccurate or incomplete PPI
 - A copy of your consent form
 - A copy of your HMIS records; and
 - A current list of participating organizations that have access to your HMIS data.
- Aggregate or statistical data that is released from the HMIS database will not disclose any of your PPI.
- You have the right to file a grievance against any organization whether or not you sign this consent.
- You are not waiving any rights protected under Federal and/or Texas law.

Right to Make Corrections

If you believe that your PPI in HMIS is incorrect or incomplete, you have the right to request a correction. To ask for either of these changes, send a written request, including the reason why you believe the information is incorrect or incomplete, to the HMIS Administrator of the organization that entered the information into HMIS. The organization may turn down your request if the information:

- Was not created by the organization you are requesting the change from;
- Is not part of the information that you would be allowed to look at and copy;
- Is related to another individual;
- Is found to be correct and complete.
- Is otherwise protected by law.

However, if your request for correction is denied, you have the right to request that the following language is entered next to a particular entry: “The participant disputes the accuracy of this entry.”

SIGNATURE AND ACKNOWLEDGEMENT

Your signature below indicates that you have read (or been read) this client consent form, have received answers to your questions, and you freely consent to have your information, and that of your minor children (if any), entered into the HMIS database. You also consent to share your information with other Participating Organizations as described in this consent form.

I consent to sharing my photograph. (Check here)

Client Name: _____ DOB: _____ Last 4 digits of SS _____

Signature _____ Date _____

Head of Household (Check here)

Minor Children (if any):

Client Name: _____ DOB: _____ Last 4 digits of SS _____ Living with you? (Y/N)

Client Name: _____ DOB: _____ Last 4 digits of SS _____ Living with you? (Y/N)

Client Name: _____ DOB: _____ Last 4 digits of SS _____ Living with you? (Y/N)

Print Name of Organization Staff

Print Name of Organization

Signature of Organization Staff

Date

Appendix D: Privacy Notice

EPCH HOMELESS MANAGEMENT INFORMATION SYSTEM (HMIS) PRIVACY NOTICE

THIS PRIVACY NOTICE EXPLAINS UNDER WHAT CIRCUMSTANCES WE MAY SHARE AND DISCLOSE YOUR INFORMATION FROM THE EPCH HMIS. THIS NOTICE ALSO EXPLAINS YOUR RIGHTS REGARDING YOUR CONFIDENTIAL INFORMATION.

PLEASE READ IT CAREFULLY.

(Organization Name Here) collects and shares information about individuals who access our services. The information is confidentially stored in a local electronic database called the El Paso Coalition for the Homeless Management Information System (EPCH HMIS). The EPCH HMIS securely records information (data) about persons accessing housing and homeless services within El Paso County/City.

We ask for your permission to share confidential personal information that we collect about you and your family. This confidential information is referred to as Protected Personal Information (PPI). We are required to protect the privacy of your PPI by complying with the privacy practices described in this Privacy Notice.

Why We Collect and Share Information

The information we collect and share in the HMIS helps us to efficiently coordinate the most effective services for you and your family. It allows us to complete one universal intake per person; better understand homelessness in your community; and assess the types of resources needed in your local area.

By collecting your information for HMIS, we are able to generate statistical reports requested by the Department of Housing and Urban Development (HUD).

The Type of Information We Collect and Share in the HMIS

We collect and share both PPI and general information obtained during your intake and assessment, which may include but is not limited to:

- Name and contact information
- Social security number
- Birthdate
- Demographic information such as gender and race/ethnicity
- History of homelessness and housing (including current housing status and where and when services have been accessed)

- Self-reported medical history including any mental health and substance abuse issues
- Case notes and services
- Case manager's contact information
- Income sources and amounts; and non-cash benefits
- Veteran status
- Disability status
- Household composition
- Emergency contact information
- Domestic violence history
- Photo (optional)

How Your Personal Information Is Protected in the HMIS

Your information is protected by passwords and encryption technology. Each HMIS user and Participating Organizations must sign an agreement to maintain the security and privacy of your information. Each HMIS user or Participating Organizations that violates the agreement may have access rights terminated and may be subject to further penalties.

How PPI May Be Shared and Disclosed

Unless restricted by other laws, the information we collect can be shared and disclosed under the following circumstances:

- To provide or coordinate services.
- For payment or reimbursement of services for the Participating Organizations.
- For administrative purposes, including but not limited to HMIS Administrator(s) and developer(s), and for legal, audit personnel, and oversight and management functions.
- For creating de-identified PPI.
- When required by law or for law enforcement purposes.
- To prevent a serious threat to health or safety.
- As authorized by law, for victims of abuse, neglect, or domestic violence.
- For academic research purposes.
- Other uses and disclosures of your PPI can be made with your written consent.

Providing Your Consent for Sharing PPI in the HMIS

If you choose to share your PPI in the EPCH HMIS, we must have your written consent.

Exception: In a situation where we are gathering PPI from you during a phone screening, street outreach, or community access center sign-in, your verbal consent can be used to share your information in HMIS. If we obtain your verbal consent, you will be requested to provide written consent during your initial assessment. If you do not appear for your initial assessment, your information will remain in HMIS until you revoke your consent in writing.

You have the right to receive services even if you do not consent to share your PPI in the EPCH HMIS.

How to Revoke Your Consent for Sharing Information in the HMIS

You may revoke your consent at any time. Your revocation must be provided either in writing or by completing the *Revocation of Consent* form. Each Participating Organization that entered information into HMIS will continue to have access to your PPI, but the information will no longer be available to any other Participating Organization.

Your Rights to Your Information in the HMIS

You have the right to receive the following, no later than five (5) business days of your written request:

- A correction of inaccurate or incomplete PPI;
- A copy of your consent form;
- A copy of the EPCH HMIS Privacy Notice;
- A copy of your HMIS records; and
- A current list of Participating Organizations that have access to your HMIS data.

You can exercise these rights by making a written request to this organization.

Right to Make Corrections

If you believe that your PPI in HMIS is incorrect or incomplete, you have the right to request a correction. To ask for either of these changes, send a written request, including the reason why you believe the information is incorrect or incomplete, to the HMIS Administrator of the organization that entered the information into HMIS. The organization may turn down your request if the information:

- Was not created by the organization you are requesting the change from;
- Is not part of the information that you would be allowed to look at and copy;
- Is related to another individual;
- Is found to be correct and complete.
- Is otherwise protected by law.

However, if your request for correction is denied, you have the right to request that the following language is entered next to a particular entry: “The participant disputes the accuracy of this entry.”

Your Privacy Rights Regarding Your Information in the HMIS

If you believe your privacy rights have been violated, you may send a written grievance to this organization. You will not be retaliated against for filing a grievance.

If your grievance is not resolved to your satisfaction, you may send a written grievance appeal to your CoC Lead.

Amendments to this Privacy Notice

The policies in this notice may be amended at any time. These amendments may affect information obtained by this organization before the date of the change. Amendments regarding use or disclosure of PPI will apply to information (data) previously entered in HMIS, unless otherwise stated. All amendments to this privacy notice must be consistent with the requirements of the federal HMIS privacy standards. This organization must keep permanent documentation of all privacy notice amendments.

Appendix E: Note Regarding Collection of Personal Information

EPCH

HOMELESS MANAGEMENT INFORMATION SYSTEM (HMIS)

NOTE REGARDING COLLECTION OF PERSONAL INFORMATION

We collect personal information directly from you for reasons that are discussed in our privacy statement. We may be required to collect some personal information by law or by organizations that give us money to operate this program. Other personal information that we collect is important to run our programs, to improve services for homeless persons, and to better understand the needs of homeless persons. We only collect information that we consider to be appropriate.

A Privacy Notice is available upon request.

Appendix F: Revocation of Consent

**EPCH
HOMELESS MANAGEMENT INFORMATION SYSTEM (HMIS)
REVOCATION OF CONSENT**

By signing below, I revoke my consent to share my Protected Personal Information (PPI) in the EPCH HMIS. I understand that each Participating Organization that entered information into HMIS will continue to have access to that information, but the information will no longer be available to any other Participating Organization.

Please provide this form to any Participating Organization that may have entered your PPI into the EPCH HMIS.

Client Name: _____ DOB: _____ Last 4 digits of SS _____

Signature _____ Date _____

- Check here and fill out the information below if you are requesting that this revocation of consent applies to your dependent(s).

Please note: Each consenting adult must fill out a separate Revocation of Consent form.

Client Name: _____ DOB: _____ Last 4 digits of SS _____

Client Name: _____ DOB: _____ Last 4 digits of SS _____

Client Name: _____ DOB: _____ Last 4 digits of SS _____

Client Name: _____ DOB: _____ Last 4 digits of SS _____

Print Name of Organization

Print Name of Organization Staff

Signature of Organization Staff

Date

Appendix G: Grievance Form

**EPCH
HOMELESS MANAGEMENT INFORMATION SYSTEM (HMIS)
GRIEVANCE FORM**

If you feel a violation of your rights as an HMIS client has occurred or you disagree with a decision made about your “Protected HMIS Information” you may complete this form. Complete this form only after you have exhausted the grievance procedures at your organization. **It is against the law for any organization to take retaliatory action against you if you file this grievance. You can expect a response within 30 days via the method of your choice.**

Grievances must be submitted in writing to:

[Enter Address]

Date of offense: _____

Name of Individual who
violated your privacy rights.

Name of Organization who
violated your privacy rights.

Brief description of grievance (what happened):

Best way to contact you:

Your name:

Your phone:

Your mailing address:

CoC response date:

Recommendation to Organization:

We collect personal information directly from you for reasons that are discussed in our privacy statement. We may be required to collect some personal information by law or by organizations that give us money to operate this program. Other personal information that we collect is important to run our programs, to improve services for homeless persons, and to better understand the needs of homeless persons. We only collect information that we consider to be appropriate.

Appendix H: Client's Rights Brochure

For Further Homeless Provider Information and Assistance



EPCH Homeless Management Information System (HMIS)

Leveraging technology in a respectful and appropriate manner, HMIS will assist homeless providers, persons experiencing a housing crisis, and policy advocates to end homelessness in the El Paso County/City geographic area.

The EPCH is dedicated to providing the best possible, highest quality HMIS to enhance the Continuum of Care for persons experiencing homelessness.

Specifically, HMIS will:

- o Enable providers to **track services, report outcomes, and manage** client data using accessible and user-friendly technology
- o Enhance the ability of policy makers and advocates **to gauge the extent of homelessness and plan services** appropriately throughout the El Paso County/City Geographic Area
- o Ensure persons experiencing a housing crisis receive **streamlined referral, coordinated services, and speedy access** to essential services and housing



Homeless Management Information System (HMIS)

Client Rights & Explanation of Data Uses

For more information, contact the
HMIS Administrative Office

Client Rights

Common Client Questions:

Who can access my information?

- Only staff who work directly with clients or who have administrative responsibilities can look at, enter, or edit client information, including all authorized organizations participating in the El Paso Continuum of Care.

Who will receive my information?

- No information will be released to another individual without your consent.
- Information is stored in an encrypted central database. Only organizations that have signed an HMIS Participating Organization Agreement will have access to HMIS data.

Don't I have a right to privacy?

- Clients do have the right to privacy, and also the right to confidentiality. You are entitled to a copy of the privacy notice upon request.
- Clients have the right to know who has modified their HMIS record.
- You also have the right to request access to your HMIS client records, printed copy of this data, and access to available audit reports. You may not see other clients' records, nor may they see your information.

What if I don't want to provide information?

- Clients have the right not to answer any questions, unless entry into a program requires it.

What if I believe my rights have been violated?

- Clients have the right to file a grievance with the organization or with the HMIS Administrative Office. Grievances must be filed through written notice. Clients will not be retaliated against for filing a complaint.

Grievance

If you feel a violation of your rights as a client has occurred, please contact your organization.

The EPCH HMIS Administrative Office can be notified of violations through written notice.

All participating organizations are responsible for ensuring that security procedures are followed and client rights are respected throughout the organization's HMIS participation.

HMIS

What Is HMIS?

The Homeless Management Information System (HMIS) is a web-based information system. Organizations that serve homeless and at-risk individuals in the El Paso County/City need to compile information about the persons they serve.

Why Gather and Maintain Data?

HMIS will gather and maintain unduplicated statistics on a regional level to provide a more accurate picture of our region's homeless and at-risk population. HMIS will also help us understand client needs, help organizations plan appropriate resources for the clients they serve, inform public policy in an attempt to end homelessness, streamline and coordinate services and intake procedures to save client's

Consent

Written Client Consent

Each client must complete a Client Consent to Share Information Agreement allowing release of demographic information to the HMIS. Clients will be required to complete a signed form to be kept on file with the service provider. A copy will be provided to the client.

