

Homeless Management Information System (HMIS) Policies and Procedures Los Angeles HMIS Collaborative

Continuum of Care HMIS Leads:
Los Angeles Homeless Services Authority
City of Pasadena
City of Glendale
City of Long Beach



Table of Contents

HMIS LEAD AGENCIES CONTACT INFORMATION	4
PROJECT SUMMARY	5
BACKGROUND	5
LA HMIS COLLABORATIVE	6
MISSION STATEMENT	6
VISION	6
LA HMIS SOFTWARE	7
1. ROLES AND RESPONSIBILITIES	8
1.1 CONTINUUMS OF CARE (CoCs) / COLLABORATIVE PARTICIPANTS	8
1.2 LA HMIS COLLABORATIVE	8
1.3 HMIS LEAD	9
1.4 LA HMIS IMPLEMENTATION MANAGER	10
1.5 HMIS PARTICIPATING ORGANIZATION.....	10
1.6 ORGANIZATION ADMINISTRATOR.....	11
1.7 HMIS END USER.....	12
2. IMPLEMENTATION POLICIES AND PROCEDURES.....	13
2.1 HMIS ORGANIZATION AGREEMENT REQUIREMENT	13
2.2 HMIS USER AGREEMENT REQUIREMENT	13
2.3 DATA COLLECTION REQUIREMENTS.....	13
2.4 TECHNICAL AND SECURITY STANDARDS	14
2.5 MAINTENANCE OF ONSITE COMPUTER EQUIPMENT	15
2.6 HMIS TECHNICAL SUPPORT PROTOCOL.....	15
2.7 SYSTEM AVAILABILITY.....	16
2.8 PARTICIPATION FEES	16
2.9 COMPUTER EQUIPMENT AND SUPPLIES.....	16
3. SECURITY POLICIES AND PROCEDURES	17
3.1 USER AUTHENTICATION	17
3.2 PASSWORDS	17
3.3 EXTRACTED DATA	18
3.4 HARDWARE SECURITY MEASURES.....	18
3.5 BACKUP AND RECOVERY PROCEDURES.....	19
3.6 SECURITY REVIEW.....	19
3.7 SECURITY VIOLATIONS AND SANCTIONS	20
4. OPERATIONAL POLICIES AND PROCEDURES.....	22
4.1 USER ACCESS LEVELS.....	22
4.2 TRAINING.....	22
4.3 USER GUIDE	23
4.4 CLIENT CONSENT TO SHARE INFORMATION AND CONFIDENTIALITY	23
4.5 REVOCATION OF CONSENT	24

4.6	DATA SHARING	25
4.7	CLIENT RECORD ACCESS.....	25
4.8	CLIENT GRIEVANCE	25
5.	DATA POLICIES AND PROCEDURES	27
5.1	DATA QUALITY.....	27
5.2	DATA USE AND DISCLOSURE	28
5.3	DATA RELEASE	29
5.4	DATA MIGRATION	29
6.	CUSTOMER PORTAL POLICIES AND PROCEDURES.....	31
6.1	IDENTITY VERIFICATION	31
6.2	ACCOUNT ACCESS	31
6.2	ACCOUNT REVOCATION AND REINSTATEMENT	32
7.	TERMINOLOGY	33
8.	APPENDICES	35
	APPENDIX A: HMIS PARTICIPATING ORGANIZATION AGREEMENT.....	36
	APPENDIX B: HMIS USER AGREEMENT	40
	APPENDIX C: CONSENT TO SHARE PROTECTED PERSONAL INFORMATION.....	43
	APPENDIX D: PRIVACY NOTICE	47
	<i>How Your Personal Information Is Protected in the HMIS.....</i>	<i>48</i>
	<i>How to Revoke Your Consent for Sharing Information in the HMIS.....</i>	<i>49</i>
	APPENDIX E: NOTE REGARDING COLLECTION OF PERSONAL INFORMATION.....	51
	APPENDIX F: REVOCATION OF CONSENT.....	52
	APPENDIX G: GRIEVANCE FORM.....	53
	APPENDIX H: CLARITY ACCESS ROLES MATRIX.....	54
	APPENDIX I: HMIS ACCESS POLICY	59

HMIS LEAD AGENCIES CONTACT INFORMATION

CoC Code	CoC Area	HMIS Lead Contact Information
CA-600	Los Angeles City & County	Los Angeles Homeless Services Authority (LAHSA) 707 Wilshire Boulevard, 10th Floor, Los Angeles, CA 90017 Tel: (213) 683-3333 Fax: (213) 892-0093 TTY: (213) 553-8434 Web: http://hmis.lahsa.org/ HMIS Support: HMISSupport@lahsa.org IT Hardware Support: ITSupport@lahsa.org
CA-606	City of Long Beach	City of Long Beach Continuum of Care 1500 Hughes Way Suite C-300 Long Beach, CA 90810 Tel: (562) 570-4454 HMIS Coordinator: Angela.diaz@longbeach.gov HMIS Support: LBHMIS@longbeach.gov
CA-607	City of Pasadena	City of Pasadena Continuum of Care 649 North Fair Oaks Avenue, Pasadena, CA 91103 Tel: (626) 744-6701 Fax: (626) 744-8340 HMIS Program Assistant: dcole@CityofPasadena.net HMIS Program Assistant: joreillyjones@CityofPasadena.net
CA-612	City of Glendale	City of Glendale Continuum of Care 141 North Glendale Avenue, Glendale, CA 91209 Tel: (818) 550-4474 Fax: (818) 548-3724 HMIS Support: HMIS@Glendaleca.gov

In addition to serving as the HMIS Lead for CA-600, LAHSA is also the HMIS implementation manager for the LA HMIS implementation as a whole. Please see section 1 for more details on roles and responsibilities.

LAHSA HMIS Training Website
<http://training.lahsa.org/>

Clarity HMIS Website
<https://la.clarityhs.com/>

PROJECT SUMMARY

Background

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

A Homeless Management Information System (HMIS) is the information system designated by a local 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 experiencing homelessness or at risk of homelessness. HMIS is a valuable resource because of its capacity to integrate unduplicated client data across projects in a community. Aggregate HMIS data can be used to understand the size, characteristics, and needs of the population experiencing homelessness 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 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)
 - Substance Abuse and Mental Health Services Administration (SAMHSA) Projects for Assistance in Transition from Homelessness (PATH) Program
 - Family and Youth Services Bureau (FYSB) Runaway and Homeless Youth (RHY) Program
- U.S. Department of Housing and Urban Development (HUD)
 - Emergency Solutions Grant (ESG) Program
 - Continuum of Care (CoC) Program
 - Youth Homelessness Demonstration Program (YHDP)
- U.S. Department of Veterans Affairs (VA)
 - Supportive Services for Veteran Families (SSVF) Program

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

The [HMIS Data Standards](#) provide communities with baseline data collection requirements developed by each of these federal partners.

LA HMIS is a response to the HUD mandated implementation of a Homeless Management Information System (HMIS) database. The LA 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 LA HMIS implementation is overseen by the LA HMIS Collaborative.

LA HMIS Collaborative

Under the guidance of the LA HMIS Collaborative, service providers are expected to participate in the LA HMIS to support local data collection, service, and planning functions within its jurisdiction. The LA Collaborative is comprised of four Continuums of Care (CoC):

1. City of Glendale
2. City of Pasadena
3. City of Long Beach
4. Los Angeles City/County

The LA Collaborative brings the following advantages:

- Comprehensive, consistent, coordinated provision of services between CoCs to meet the specific needs of persons experiencing and at-risk of homelessness.
- Enhanced understanding of needs, service usage, and effectiveness using regional data and reports.

Mission Statement

The LA HMIS Collaborative will use the LA HMIS to advance the provision of quality services for persons who are experiencing homelessness or at-risk of homelessness, to improve data collection, and promote more responsive policies to prevent and end homelessness in Los Angeles County.

Vision

The LA HMIS Collaborative 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, the LA 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 Los Angeles.

LA HMIS Software

In addition to meeting federal reporting requirements, LA HMIS is a comprehensive data management system that allows the LA Collaborative and users to mobilize 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.

LA HMIS includes the following components:

- Advanced security features
- Bed tracking and assignment feature
- Client demographic data collection
- 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 Continuums of Care (CoCs) / Collaborative Participants

CoCs participating in the LA HMIS implementation retain decision-making authority for all HMIS-related responsibilities of each CoC as described in the CoC Program interim rule and other guidance published by HUD.

HMIS-related responsibilities of each CoC include:

- Designate a single Homeless Management Information System (HMIS) for the geographic area.
- Designate an eligible applicant to manage the Continuum's HMIS, which will be known as the HMIS Lead.
- Review, revise, and approve a privacy plan, security plan, and data quality plan for the HMIS. (Note: privacy plan and security plan are designated to the LA HMIS Collaborative. Each CoC maintains its own data quality plan.)
- Ensure consistent participation of recipients and subrecipients in the HMIS.
- Ensure HMIS is administered in compliance with requirements prescribed by HUD.
- Appoint two (2) members to the LA HMIS Collaborative in accordance with the Los Angeles HMIS Collaborative Memorandum of Understanding.

1.2 LA HMIS Collaborative

The Collaborative will be responsible for the organization and management of the LA HMIS, including the HMIS Lead organizations, participating CoCs and their governing bodies, and contributing providers within each of the CoCs on all matters regarding homeless data management. These activities address the common HMIS policy and governance issues that collectively affect HMIS end users and other HMIS partners. Additionally roles and responsibilities of the LA HMIS Collaborative, and the entities that it comprises, can be found in the LA HMIS Collaborative Memorandum of Understanding.

The activities of the LA HMIS Collaborative include:

- Develop, review, and update HMIS Policies and Procedures (P&Ps), Privacy Policy, and any other relevant documents that support the LA HMIS at the systemwide level.
- Monitor compliance of system with HUD and other mandates.
- Ensure the LA HMIS meets the needs of providers, end users, and participating CoCs.
- Discuss major HMIS issues, including vendor/software performance, system inefficiencies, privacy, and data sharing.
- Provide feedback to HMIS Leads and CoCs on emergent issues.
- Serve as point of communication among CoCs for HMIS-related issues.

- Serve as approval body for system-level HMIS changes that would affect all CoCs in the implementation.
- Define roles and responsibilities of HMIS Leads, end users, decision-making parties, and other HMIS partners as they pertain to joint HMIS governance.

The collective activities of the LA HMIS Collaborative are limited to those items that affect HMIS across the implementation as a whole. Therefore, the following activities are not included in the activities of the Collaborative:

- Use of local data for CoC-specific reporting.
- Management of the costs associated with CoC-specific system features, modifications, or modules that do not affect the multi-CoC HMIS implementation as a whole.
- Selection of the HMIS Lead by each CoC.
- Creation and management of an HMIS budget and staffing plan for each CoC.

1.3 HMIS Lead

As a multi-CoC HMIS implementation, LA HMIS involves coordination among several different organizations serving as HMIS Lead for their respective CoCs. Organizations designated as HMIS Leads retain all responsibilities of that designation as prescribed by HUD and their CoC's governance charter. In general, these include:

- Submission of annual HMIS application to HUD.
- Receipt and management of HMIS CoC grant.
- Submission of annual HMIS APR.
- Submission of required annual federal reports for CoCs.
- Management of the CoC's policy for collection of agency/end user fees.
- Entering into HMIS system administration MOU or service contract (as applicable).
- Review of CoC-level and project-level data quality benchmarks for timeliness, completeness, accuracy, and consistency.
- Conduct monitoring of end users to ensure compliance with HMIS plans, policies, and procedures.
- Collaborate with the LA HMIS Collaborative to develop forms and documents as needed.
- Ensure the training needs of HMIS End Users ("Users") are met, in collaboration with the LA HMIS Implementation Manager

HMIS Leads are also responsible for all activities identified in the [HMIS System Administrator Checklist](#), unless otherwise delegated to other parties in this charter or each CoC's governance charters. In general, HMIS Leads are responsible for the following system administration activities:

- Managing project setup tasks.
- Establishing and managing data entry workflows, features, and functionality.
- Providing troubleshooting/technical assistance via service desk activities and other modalities.
- Preparing federal, state, and local reports, including managing data quality cleanup activities necessary to ensure accuracy of reporting.
- Merging duplicate client records.

Additionally, each HMIS Lead employs one or more HMIS Administrators, who are 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.
- Communicating system-related information to Participating Organizations.
- Developing and modifying reports for Users.

1.4 LA HMIS Implementation Manager

In addition to its duties as HMIS Lead for CA-600, LAHSA functions as the HMIS Implementation Manager for the LA HMIS implementation as a whole. Its responsibilities include:

- Coordinating with the HMIS vendor to ensure LA HMIS maintains operational functionality for all participating CoCs.
- Requesting vendor upgrades or customizations when needed.
- Reviewing updates to HMIS software related to the [HMIS Data Standards](#) for correctness and completeness.
- Developing shared forms and documents as needed.
- Developing HMIS training materials, training new HMIS end users, and offering refresher/retraining opportunities as outlined in the LA HMIS training plan for HMIS Participating Organizations that operate within any CoC holding a separate training agreement with LAHSA.

1.5 HMIS Participating Organization

HMIS participating organizations are agencies operating within a CoC that provide services to individuals and households experiencing homelessness and record, use, or process data for an HMIS. In the 2004 Data and Technical Standards Final Notice, participating organizations

are referred to as covered homeless organizations (CHOs). For the LA HMIS implementation, participating organizations will:

- Ensure compliance with the standards for CHOs outlined in the 2004 Data and Technical Standards, including HMIS privacy and security standards outside of HMIS such as security of workstations and paper forms.
- Adhere to all requirements and agreements outlined in the agency's Collaborative Participation Agreement.
- Maintain documentation of HMIS access and training requirements for all associated end users.
- Notify the HMIS Lead of any breaches/violations of HMIS policies or end of a users' employment within the timeframe specified in the HMIS Policies and Procedures Manual
- 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 LA HMIS to ensure adherence to the Policies & Procedures described in this document.
- Notify the HMIS Lead of the agency's selected Organization Administrator and communicate any changes to the Organization Administrator's contact information within 3 days of a change.

1.6 Organization Administrator

An Organization Administrator is defined as a single point-of-contact, established by each HMIS participating organization, who is responsible for:

- Serving as the primary contact between Users and HMIS Administrator.
- Providing technical support and escalating unresolved issues to the HMIS Administrator.
- Notifying all members of their organization of any system-wide changes and other relevant information.
- Conduct training for Users, based on local region policies.
- Notifying the HMIS Administrator (from the relevant HMIS Lead) of User changes on the day the change occurs.
- Monitoring compliance with standards of confidentiality and data collection, entry, and retrieval.
- Ensuring that all authorized Users complete training before being granted access to the system, including adherence and understanding of the HMIS User Agreement.
- Ensuring organizational adherence to the Policies and Procedures.
- Ensuring project-level data quality according to the terms of the organization's Collaborative Participation Agreement and any associated HMIS data quality plan.
 - Detecting and responding to violations of the Policies and Procedures.

1.7 HMIS End User

Individuals who have rights to view and/or enter client-level data, otherwise known as “HMIS end users” or “users,” are granted access to HMIS by approval of the HMIS Lead designated for the CoC to which they are associated, and in accordance with the HMIS Policies and Procedures Manual. HMIS end users will:

- Uphold the terms of End User Agreement between the end user and corresponding HMIS Lead.
- Maintain compliance with all relevant HMIS policies and procedures as outlined in the LA HMIS Policies & Procedures Manual, adhering to standards for data collection, entry, privacy, and security.
- Uphold any additional responsibilities as assigned by the CoC for which the User has been provided access.

NOTE: Staff of agencies classified as victim service providers (VSPs) are prohibited from entering information into HMIS in accordance with the Violence Against Women Act (VAWA).

2. IMPLEMENTATION POLICIES AND PROCEDURES

2.1 HMIS Organization Agreement Requirement

Policy:

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

Procedure:

- An original, scanned, or a digitally signed HMIS Participating Organization Agreement must be presented to the HMIS Administrator before program implementation or user training on the LA HMIS.
- After HMIS Participating Organization Agreement is signed, the HMIS Administrator will train Users to use the LA HMIS.
- A username and password will be granted to Users after required training is completed and the HMIS User Agreement is signed.

2.2 HMIS User Agreement Requirement

Policy:

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

Procedure:

- The HMIS Administrator will provide the User an HMIS User Agreement for signature after required training is completed.
- The HMIS Administrator will collect and maintain HMIS User Agreements of all Users.
- The HMIS Administrator must provide HMIS Users with a written copy of updates and/or changes to the User Agreement, within 3 business days of Participating Organizations being informed of the updates from the HMIS Administrator.
- HMIS Users who violate the User Agreement must be 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.

2.3 Data Collection Requirements

Policy:

Participating Organizations will collect and verify required data elements for all clients served by their programs.

Procedure:

- Participating Organizations must enter data into the system within 3 days of collecting the information.
- Users must collect all the universal data elements set forth in the current version of the [HMIS Data Standards Manual](#).
Users must also collect all the program-specific data elements at project start and exit set forth in the current version of the [HMIS Data Standards Manual](#).
- These standards are already required fields in the LA HMIS. For other funder-specific program data elements, refer to the most recent federal partner program manual.

Note: while these are the minimal standards per HUD and the federal partners, each 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 LA HMIS.

Procedure:

- Clarity Human Services, the software designated as the LA HMIS, takes advantage of the latest in web technologies. For both security and compatibility, a Participating Organization's local IT Staff should ensure all workstations are outfitted with the latest version of the web browser utilized by Users.
- The following web browsers are [supported by Clarity](#):
 - Microsoft Edge
 - 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 LA HMIS.
- All operating systems should have the latest Service Pack or official update applied. Network design should allow for uninterrupted communication between application, database, report, and batch servers. Communication should be capable using the following standard protocols TCP/IP, WIN, DNS, Named Pipes, and NetBIOS. All communication between servers should be designed to be performed on Local Area Network.
- For security purposes, all computers must have the following:

- An updated and adequate firewall protection.
- Virus protection software in which virus definitions must be updated regularly.

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 on.
 - 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:

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

Procedure:

- Users should first seek technical support from the Organization Administrator.
- If more expertise is required to further troubleshoot the issue, Organization Administrator will contact the HMIS Help Desk of the relevant CoC.
- The HMIS Administrator Support Hours are Monday through Friday (excluding holidays) from 9:00 am to 5:00 pm.
- The Organization Administrator will provide sufficient issue details where possible (or help recreate the problem by providing all information, screenshots, reports, etc.) for the HMIS Administrator to recreate the problem.
- The HMIS Administrator will try to respond to all email inquiries and issues within 3 business days, but support load, holidays, and other events may impact response time.
- The HMIS Administrator will submit a ticket to the HMIS vendor if the issue cannot be resolved by the HMIS Administrator.

- For LAHSA HMIS/IT Technical Support, see the Supplemental Policies for LAHSA Only.

2.7 System Availability

Policy:

The LA HMIS will be available to Users at a minimum of 97.5% of the year. The HMIS vendor and the HMIS Lead Agency will inform users in advance of any unplanned interruption in service.

Procedure:

- The HMIS vendor will communicate to all HMIS Administrators at each CoC and backup 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 LA HMIS accessibility is disabled system-wide, the HMIS Administrators will analyze and determine the problem.
- The HMIS Administrator will work with the HMIS vendor to repair the problem.
- The HMIS Administrators will send email communication to the Organization Administrators within 2 hours of issue discovery and inform them of anticipated interruptions to system availability.

2.8 Participation Fees

Policy:

Each Continuum of Care reserves the right to charge a participation fee to use the system.

Procedure:

- Consult local HMIS Lead regarding fees.

2.9 Computer Equipment and Supplies

Policy:

Each Continuum of Care may provide computer equipment and supplies at the HMIS Lead Agency's discretion.

Procedure:

- Consult local HMIS Lead Agency regarding computer equipment and supplies policies.

3. SECURITY POLICIES AND PROCEDURES

3.1 User Authentication

Policy:

LA HMIS can only be accessed with a valid username and password combination. The HMIS Administrator will provide unique username and initial password for eligible Users after completion of required training, signing the HMIS User Agreement, and receipt of these Policies and Procedures.

Procedure:

- The Participating Organization will determine which of their employees should have access to the LA HMIS. User access will be granted only to those individuals whose job functions require legitimate access to the system.
- A proposed User must complete the required training and demonstrate proficiency in use of the system.
- A proposed User must sign the HMIS User Agreement stating that they have received training, will abide by the HMIS Policies and 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.
- HMIS Administrators will be responsible for the distribution, collection, and storage of the signed HMIS User Agreements and distribution of these Policies and Procedures.
- The HMIS Administrator will assign new Users with a username and an initial password.
- Sharing of usernames and passwords is considered a breach of the HMIS User Agreement and is not permitted.
- An Organization Administrator is required to notify the HMIS Administrator on the day when a User leaves employment with the organization or no longer needs access.
- HMIS Administrator will terminate access upon notification of the Organization Administrator within one (1) business day.

3.2 Passwords

Policy:

User will have access to the LA HMIS via a username and password. Passwords will be reset every 180 days. Users will ensure their password is maintained confidentially.

Procedure:

- The HMIS Administrator will provide new Users with a unique username and temporary password after required training is completed.
- Upon initial login, user will be required to create a new 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, \$, #, %).

- For security purposes, the Forced Password Change (FPC) will occur every 180 consecutive days and the User will be prompted to enter a new password. Users may not use the same password consecutively.
- After 60 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 if they do not elect to continue their session.
- User can reset their own password from the log-in screen.
- Access permission will be revoked after the User unsuccessfully attempts to log on three times. The User will be unable to gain access until they reset their password or after one hour.

3.3 Extracted Data

Policy:

Users will maintain the security of any client data extracted from the LA 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 LA 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.
- Personally 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 LA 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 LA HMIS access.
- Virus definitions 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.

- The Organization Administrator will ensure that computers maintain security specifications.

3.5 Backup and Recovery Procedures

Policy:

The HMIS vendor will perform regular schedule backups of the system to prevent the loss of data. Multiple levels of backup and storage will be used for key data and files within the LA HMIS.

Procedure:

- The HMIS vendor's designated hosting company will perform data backup procedures in the following manner:
 1. Daily – resulting in a seven (7) day backup;
 2. Weekly – resulting in a four (4) or five (5) week backup; and
 3. Monthly – during the term of contract with the HMIS vendor.
- The HMIS vendor shall maintain an off-site storage of tapes in fireproof containers.
- The HMIS vendor recovery procedures will be undertaken on a “best efforts” basis to achieve the following response times:
 1. Data Loss – confirmation response and recovery implementation within 4 hours of reported data loss by the local HMIS Administrator
 2. LA HMIS source code corruption and/or user functionality loss – confirmation response within 4 hours and full initiation of recovery procedures within 24 hours of reported disruption by the local HMIS Administrator.
 3. Disaster – notification within 4 hours and recovery implementation to fully re-establish operations within 5 business days.

3.6 Security Review

Policy:

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

Procedure:

- The HMIS Lead 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 violating security protocols of their Participating Organization’s procedures or the HMIS Policies and Procedures will be sanctioned accordingly. Users found in violation may be temporarily or permanently suspended from HMIS based on an investigation of the violations. All Users must report potential violations of any security protocols described in these Policies and Procedures. Depending on the severity of the violation(s), the CoC and/or Implementation Manager reserves the right to immediately and permanently revoke access from a User without the complete three warnings. A monthly report will be provided to the LA HMIS Collaborative of any violations of LA HMIS security policies.

Procedure:

- Users are required to report suspected instances of noncompliance and/or security violations to the Organization Administrator or HMIS Administrator immediately upon discovery.
- The Organization Administrator or HMIS Administrator will investigate potential violations.
- Any User found to be in violation of security protocols will be sanctioned in accordance with the table below. Sanctions may include but are not limited to suspension of system privileges and revocation of system privileges.

Warnings and Actions:

Warnings	Result
First Warning	LAHSA's HMIS Admin will inform the Deputy CIO of all violations, and the user will be notified in writing to ensure the offense doesn't happen again.
Second Warning	Temporary suspension from HMIS with mandatory refresher training ensures each end user understands the HMIS Security procedures and expectations.
Third Warning	After providing training, the user continues violating the HMIS Access Policy. Permanent suspension from HMIS access across the CoC will be enacted. The suspension cannot be appealed.

Additionally, individual Users and/or Participating Organizations found in violation of these policies may be referred to Los Angeles County's Fraud Hotline and/or law enforcement agencies for additional investigation and possible prosecution. The CoC reserves the right to immediately make this referral without issuing three warnings, depending on the severity of the violation(s).

All HMIS users will follow the HMIS Policies and Procedures for disclosure of client information stored in HMIS. LAHSA Risk Management will investigate egregious violations.

No identifiable client data will be released to any person, agency, or organization for any purpose without written permission from the client.

4. OPERATIONAL POLICIES AND PROCEDURES

4.1 User Access Levels

Policy:

Each User will be assigned a user access level that controls the level and type of access they have to data and functionality within the LA 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.
- Organization Administrator is required to communicate to HMIS Administrator when User's need for access changes.
- HMIS Administrator will terminate access upon notification and receipt of Termination of Employee Form from the Organization Administrator.
- 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.

Please see Clarity Access Roles Matrix on Appendix H that lists the levels of access tied to existing user roles across the LA Collaborative. This might include a role not available within any of the participating CoCs. Consult the local HMIS Lead to learn which user access levels are available, as well as other customizable roles, such as Coordinated Entry, that may be offered after consultation with and approval from the HMIS Administrator (See HMIS Lead Agencies Contact Information).

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 LA HMIS. HMIS Administrators will provide training to all Users.

Procedure:

- HMIS Administrator will provide Basic User Training to proposed Users. Organization Administrator may be trained to provide Basic User Training to support organization personnel or personnel of the other organizations in LA County, if applicable. Consult local HMIS Lead Agency (See HMIS Lead Agencies Contact Information).
- User must successfully complete the Basic User Training to demonstrate proficiency in the system and understanding of the Policies and Procedures.
HMIS Administrator will provide new User with a copy of the Policies and Procedures and HMIS Users Guide.

- HMIS Basic Training completed in one region will satisfy the training requirements in any other region in the Collaborative.
- For LAHSA Participating Organizations, see the Supplemental Policies for LAHSA Only: LAHSA Training Requirements.

4.3 User Guide

Policy:

Each User will receive a copy of the LA HMIS User Training Manual.

Procedure:

- The HMIS Administrator will create and update the user training manual as needed.
- The user training manual will contain instructions on how to use the system.
- Each User will be given a user training manual after completing training.

4.4 Client Consent to Share Information and Confidentiality

Policy:

Participating Organizations must obtain informed, signed consent prior to either sharing or accessing any client personally identifiable information (PII) in the LA HMIS. Services will not be denied if client chooses not to provide or include PII for sharing in HMIS. Personal information collected about the client should be protected. Each Participating Organization and User must abide by the terms in the HMIS Participating Organization Agreement and HMIS User Agreement.

Procedure:

- Client must sign Consent to Share Protected Personal Information (Appendix C).
- Clients that provide permission to share 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.
- A signed copy of the Consent to Share Protected Personal Information must be retained for a period of seven (7) years after the PPI was created or last changed.
- 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 in the client record. Instead, User should include a client identifier to

recognize the record in the system. In this instance, at minimum, the following data should not be entered into HMIS:

- First name
- Last name
- Social security number
- Date of birth
- 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 Health Insurance Portability and Accountability Act (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 people experiencing or at-risk of homelessness 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.

4.5 Revocation of Consent

Policy:

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

Procedure:

- HMIS Users must forward a copy of a client's *Revocation of Consent* to the HMIS Administrator within 24 hours of receipt.
- 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 Organizations that have previously provided services will still have access to clients' project enrollment and service history.

4.6 Data Sharing

Policy:

Client data (with consent) contained in LA 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.

4.7 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 will review client information with client if they request to view their HMIS data.
- No client shall have access to another client record in the system. Parental or guardian access will be decided based upon existing organization guidelines.
- Client may request that PPI be removed from the system. In response, the Organization Administrator will remove such data from record within 5 business days.
- A copy of the requested data will be provided to client within a reasonable time frame.

4.8 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 local 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 LA HMIS Policies and Procedures.
- The Participating Organization will be responsible for answering any questions and complaints regarding the LA 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 local HMIS Lead Agency.
- If the Participating Organization is unable to resolve the problem, the client must complete the Grievance Form (Appendix H) 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 local HMIS Lead Agency.
- The local HMIS Lead Agency will review and determine the need for further action.

5. DATA POLICIES AND PROCEDURES

5.1 Data Quality

Data quality refers to the timeliness, completeness, accuracy, and consistency of information collected and reported in the LA HMIS. What follows are the baseline policies and procedures for data quality. Please refer to each CoC's Data Quality Management Program for more detail.

Policy:

All data entered into the LA HMIS must meet data quality standards defined by each CoC. Users will be responsible for the quality of their data entry.

Data Timeliness:

Users must enter all universal data elements and program-specific data elements within three (3) business days of collection.

Data Completeness:

All data entered into the system must be complete, unless otherwise authorized by the HMIS Lead, following data collection standards set by the most recent HUD HMIS Data Standards.

Data Accuracy:

All data entered shall reflect the best representation of the client's real-world situation and the programs that provide housing and services.

Data Consistency:

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

Procedure:

- Participating Organizations must sign the 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.
- All data will be input into the system within three (3) business days of collection.
- The HMIS Administrator will conduct regular checks for data quality. Any patterns of error or missing data will be reported to the Organization Administrator.
- Users will be required to correct the identified data error and will be monitored for compliance by the Organization Administrator and the HMIS Administrator.
- Users may be required to attend additional training as needed.

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 LA 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 Los Angeles.
- Each of the HMIS Administrators within the LA HMIS Collaborative shall have access to their respective agencies' client data stored in the system. The Collaborative 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.
- With the exception of supporting the LA HMIS partners in troubleshooting issues that are identified and asked for support to address by the LA HMIS partners, the HMIS vendor and any authorized subcontractor shall not use or disclose data stored in the LA HMIS without expressed written permission 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 between each Continuum and the HMIS 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 LA HMIS partners will follow the data release Policies and Procedures to guide the data release of client information stored in the LA 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.
- Each Participating Organization is a steward for all data they collect and enter in the system. Organizations may release program and/or aggregate level or de-identified data for all clients to whom the organization provided services. The organization may not disclose personally identifiable client data without written permission from the client.
- Each CoC within the LA HMIS Collaborative may release aggregate or de-identified data about its own CoC at the program, sub-regional, and regional level. Aggregate or de-identified data may be released without organization permission at the discretion of the CoC. The Collaborative may develop an annual release of aggregate data in a summary report format.
- The HMIS Implementation Manager may release aggregate or de-identified data to meet system/county-wide data requests. The HMIS Implementation Manager will inform each CoC of these data requests before fulfilling them.

5.4 Data Migration

Policy:

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

Definition:

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

Data uploads (transfers): ongoing, periodic process of transferring data from an existing system to the LA 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 or uploaded data must be non-duplicated and an exact match to the existing field types of the LA 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 LA HMIS data fields may be migrated or uploaded. Data must be unduplicated prior to data migration or upload. All required fields in the LA HMIS are required for migration or upload. A data dictionary will be provided upon request.
- The HMIS Administrator will decide the appropriate data migration or upload 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 LA HMIS.
- Data uploads will be reviewed on a regular basis. If recurring issues are identified, they will be discussed and, if unresolved, used to determine if uploads will continue to be permissible.

6. Customer Portal Policies and Procedures

The LA HMIS Customer Portal is secure software that allows people experiencing homelessness to access a portion of their HMIS client records.

6.1 Identity Verification

Policy:

Clients seeking access to the Customer Portal must have their identity verified by a Participation Organization that has provided services to them.

Procedure:

- For any client seeking access to the Customer Portal, the Organization Administrator will collect a client's full name and two additional identifiers, which may include: full date of birth, Social Security Number, HMIS Unique ID, client's address, client's phone number, or other identifying information in the client's HMIS record as determined by the HMIS Administrator.
- Upon verification, Organization Administrators will notify the HMIS Administrator that corresponds with the CoC from which the client receives services.

6.2 Account Access

Policy:

The Customer Portal can only be accessed with a valid username and password combination, after identity verification provided by a Participating Organization that has provided services to the client seeking access. Clients with access to the Customer Portal are considered HMIS Users (with access limited to the Customer Portal) and must sign an HMIS User Agreement before being granted access to the Customer Portal. Clients must be age 18 or older to access the Customer Portal. Youth experiencing homelessness who are in a household without someone age 18 or older may also be provided access.

Procedure:

- After notification from the Organization Administrator, the HMIS Administrator will provide the client with training on use of the Customer Portal.
- The HMIS Administrator will provide the client an HMIS User Agreement for signature after required training is completed.
- The client must return an original, scanned, or digitally signed HMIS User Agreement to the HMIS Administrator.
- The HMIS Administrator will collect and maintain HMIS User Agreements of all clients with access to the Customer Portal.

6.2 Account Revocation and Reinstatement

Policy:

Only clients who have signed the HMIS User Agreement may access the Customer Portal.

Procedure:

- Customer Portal accounts found to have been accessed by anyone other than the authorized client will be immediately suspended by the HMIS Administrator.
- Accounts may be reinstated after retraining and identity credentials have been verified.

7. TERMINOLOGY

Aggregate Data: Data with identifying elements removed and combined from multiple sources (usually client records). 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 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: Software developer of Clarity Human Services, the designated HMIS for the LA HMIS implementation.

Clarity Human Services: The software designated as the HMIS for the LA HMIS implementation.

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

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

Database: An electronic system for organizing data so it can easily be searched and retrieved. The data within the LA HMIS is accessible through a 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.

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.

Homeless Management Information System (HMIS): A local information technology system used to collect client-level data and data on the provision of housing and services to individuals and families at-risk of and experiencing homelessness.

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 HMIS vendor. There is at least one HMIS Administrator in each CoC.

HMIS Lead: The organization designated by each CoC that manages and operates HMIS on behalf of the CoC and receives the CoC-funded HMIS grant.

HMIS User (User): An individual who has a unique user identification (ID) and directly accesses the LA HMIS to assist in data

collection, reporting, or administration as part of their job function in homeless service delivery. Users are classified as either system Users who perform administration functions for or organization Users that perform functions at the participating organization level.

HMIS Vendor: Provider of software that is designated by the CoC to operate as the community's HMIS.

Internet Protocol Address (IP Address): A unique address assigned to a user's connection based on the TCP/IP network. The Internet address is usually expressed in dot notation, e.g.: 128.121.4.5.

Internet Service Provider (ISP): A company that provides individuals or organizations with access to the internet.

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

LA HMIS: The Los Angeles Homeless Management Information System provided by the HMIS vendor and tailored for use in the LA region.

LA HMIS Collaborative Steering

Committee: Comprised of at least one representative from each of the LA HMIS Collaborative governing bodies. It is responsible for setting and overseeing policy for the regional implementation of the LA HMIS.

Network: Several computers connected to each other.

Organization Administrator: The person responsible for data management at a

Participating Organization. This person is the organization user's first line of contact for LA HMIS issues.

Participating Organization: An organization that operates a project that either contributes data to an HMIS or has direct access to personally identifying information (PII) in HMIS.

Personally Identifiable Information (PII): Any information maintained by or for a Participating Organization about a person at-risk of or experiencing homelessness that identifies, either directly or indirectly, a specific individual; can be manipulated by a reasonably foreseeable method to identify a specific individual; or can be linked with other available information to identify a specific individual.

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.

8. 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	Clarity Access Roles Matrix
Appendix I	HMIS Access Policy

Appendix A: HMIS Participating Organization Agreement

GREATER LOS ANGELES HOMELESS MANAGEMENT INFORMATION SYSTEM (LA HMIS) PARTICIPATING ORGANIZATION AGREEMENT

I. Purpose

The HMIS is a HUD-mandated information technology system that is designed to capture longitudinal client-level information about the characteristics and service needs of people at-risk of and experiencing homelessness. Client data is maintained on a central server, maintained by the HMIS vendor, which will contain all client information in an encrypted state. HMIS includes data from all participating homeless service providers and organizations in the community and captures basic descriptive information on every person served. Participation in LA HMIS allows organizations to share information with other Participating Organizations to create a more coordinated and effective delivery system, and more efficiently, effectively, and equitably serve people at-risk of and experiencing homelessness.

The LA HMIS is the secured electronic database for the Greater Los Angeles area and is a valuable resource for local communities. The LA HMIS is overseen by the LA HMIS Collaborative. The LA HMIS Collaborative consists of several separate Continuums of Care (CoCs):

- CA-600 Los Angeles City and County CoC
- CA-606 Long Beach CoC
- CA-607 Pasadena CoC
- CA-612 Glendale CoC

In addition to ensuring the LA HMIS meets HUD's baseline requirements, the LA HMIS Collaborative's goal is to provide a comprehensive case management system to advance the provision of quality services for people at-risk of and experiencing homelessness, improve data collection, and promote more responsive policies to end homelessness in the Greater Los Angeles area.

II. Agreement and Understanding

This Agreement authorizes this Participating Organization (Organization) to designate HMIS Users (User). A User is a staff person entrusted to enter Protected Personal Information (PPI) into the LA HMIS, on behalf of this Organization. To allow a User to access the LA HMIS, a User Agreement must be signed by the User, the HMIS Administrator, and this Organization's Authorized Representative.

III. Confidentiality and Informed Consent

Confidentiality: This Organization must require all Users to abide by its organization's policies and procedures; uphold all privacy protection standards established by the LA HMIS Collaborative Policies and Procedures; and comply with all relevant federal and State of California confidentiality laws and regulations that protect client records. Except where otherwise provided for by law, this Organization shall ensure that confidential client records are released with the client's written consent.

Written Consent: To obtain written consent, prior to each client's assessment, each client must be informed that the client's information will be shared in an electronic database called HMIS. The terms of the *Consent to Share Protected Personal Information* form must also be explained to each client. Clients who agree to have their PPI shared in the LA HMIS must sign the *Consent to Share Protected Personal Information* form.

Verbal Consent: Verbal consent to share PPI in the LA HMIS may be obtained during circumstances such as phone screenings, street outreach, or community access center sign-ins. Each client must be informed that their information

will be shared in the HMIS database. The terms of the *Consent to Share Protected Personal Information* form must also be explained to each client. The client's written consent must be obtained once the client appears for their initial assessment.

IV. Client's Rights

The client has a right to receive a copy of this notice at the time of request.

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 their consent form
- A copy of their HMIS records
- 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 they 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 the request if the information:

- Was not created by the organization the client is requesting the change from;
- Is not part of the information that the client 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 the request for correction is denied, the client has 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 the Organization's website
- LA HMIS is not accessible to unauthorized Users
- LA HMIS is only accessed by computers approved by the Organization
- HMIS Users are trained regarding user responsibilities and conduct
- 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 *LA HMIS User Agreement*
- HMIS Users are provided with a written copy of updates and/or changes to the User Agreement, within 3 business days of this Organization receiving the updates from the HMIS Administrator
- HMIS Users forward a copy of a client's *Revocation of Consent* to the HMIS Administrator within 24 hours of receipt.

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

VII. System Use

Computer equipment and services provided by a CoC are intended only for LA 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, operating 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

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

IX. Copyright

The LA 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 Administrator.

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 Organization 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 LA HMIS Collaborative 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 LA 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 LA HMIS agree to abide by the LA HMIS Collaborative 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 CoC and the Participating Organizations. Upon final execution, this Organization will be given access to the LA HMIS.

_____ Organization Name	_____ CoC Name
----------------------------	-------------------

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

_____ Signature	_____ Signature
--------------------	--------------------

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

Appendix B: HMIS User Agreement

Greater Los Angeles Homeless Management Information System (LA HMIS) USER AGREEMENT

I. Purpose

The LA HMIS is the secured electronic database for the Greater Los Angeles area and is a valuable resource for local communities. The LA HMIS is overseen by the LA HMIS Collaborative. The LA HMIS Collaborative consists of several Continuums of Care (CoC):

- CA-600 Los Angeles City and County CoC
- CA-606 Long Beach CoC
- CA-607 Pasadena CoC
- CA-612 Glendale CoC

In addition to ensuring the LA HMIS meets HUD's baseline requirements, the LA HMIS Collaborative's goal is to provide a comprehensive case management system to advance the provision of quality services for people at-risk of and experiencing homelessness, improve data collection, and promote more responsive policies to end homelessness in the Greater Los Angeles.

II. Agreement and Understanding

This Agreement authorizes you, an HMIS User (User), to enter Protected Personal Information (PPI) into the LA 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 LA HMIS Collaborative Policies and Procedures; and comply with all relevant federal and State of California 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 their PPI entered into the LA HMIS must sign the *Consent to Share Protected Personal Information* form.

Verbal Consent: Verbal consent to enter PPI into the LA 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 their initial assessment.

III. Client Rights

- A client may not be denied services for failure to provide consent for LA HMIS data sharing.
- A client has the right to inspect, copy, and request changes in their LA 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 their consent form;
 - A copy of their 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 a correction. To ask for either of these changes, the client will need to send a written request, including the reason why they 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 the request if the information:

- Was not created by the organization they are requesting the change from;
- Is not part of the information that they 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 their request for correction is denied, they 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 official purposes of my job responsibilities.
- 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 a 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 authorized 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 LA HMIS Collaborative Policies and Procedures in my use of HMIS. The LA HMIS Collaborative Policies and Procedures can be accessed from the CoC HMIS 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 for complying 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.
- If I have a conflict of interest in entering data within the LA HMIS, I will disclose that to my Organization's HMIS administrator. If I am a client within the LA HMIS, or if I have immediate family members within the LA HMIS, I will not access or make changes to those records.

My signature below confirms my agreement to comply with all the provisions of this Greater Los Angeles 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

DO NOT WRITE IN THIS SECTION. (FOR HMIS ADMINISTRATOR STAFF ONLY.)

HMIS Staff Name: _____ Date: _____

Date of Training: _____ Trainer: _____

HMIS User ID: _____ Date User ID Issued: _____

Appendix C: Consent to Share Protected Personal Information

Greater Los Angeles Homeless Management Information System (LA HMIS) CONSENT TO SHARE PROTECTED PERSONAL INFORMATION

The LA HMIS is a local electronic database that securely records information (data) about clients accessing housing and homeless services within the Greater Los Angeles County. 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 case notes and services
- Your case manager's contact information
- Your income sources and amounts; and non-cash benefits
- Your veteran status
- Your disability status
- Your household composition
- Your emergency contact information
- Any history of domestic violence
- 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 local 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 LA 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 California 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), shared 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

Greater Los Angeles Homeless Management Information System (LA HMIS) PRIVACY NOTICE

THIS PRIVACY NOTICE EXPLAINS UNDER WHAT CIRCUMSTANCES WE MAY USE AND DISCLOSE YOUR INFORMATION FROM THE LA 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 Greater Los Angeles Homeless Management Information System (LA HMIS). The LA HMIS securely records information (data) about persons accessing housing and homeless services within Greater Los Angeles.

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) and other federal partners.

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 Organization must sign an agreement to maintain the security and privacy of your information. Each HMIS user or Participating Organization 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 LA 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 LA 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 LA 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 the HMIS Administrator for your CoC.

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

Greater Los Angeles Homeless Management Information System (LA 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 people at-risk of and experiencing homelessness, and to better understand the needs of people at-risk of and experiencing homelessness. We only collect information that we consider to be necessary and appropriate.

A Privacy Notice is available upon request.

Appendix F: Revocation of Consent

Greater Los Angeles Homeless Management Information System (LA HMIS) REVOCATION OF CONSENT

By signing below, I revoke my consent to share my Protected Personal Information (PPI) in the LA 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 LA 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

Greater Los Angeles Homeless Management Information System (LA 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 Personal Information” in HMIS, you may complete this form. Complete this form only after you have exhausted the grievance procedures at the organization currently providing you services. **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 people at-risk of and experiencing homelessness, and to better understand the needs of people at-risk of and experiencing homelessness. We only collect information that we consider to be appropriate.

Appendix H: Clarity Access Roles Matrix

Client Profile Pages	Description	Clarity Access Roles				Admin Roles
		Limited Read	Basic User	Agency Admin	CES Lead/Matcher	System Administrator
History	History of the Client's service, enrollment, assessment history from anywhere.	X	X	X	X	X
Services	Provide Services not connected to programs		X	X	X	X
Programs	Enroll into programs and see history of enrollments (Depending on access level)		X	X	X	X
Public Alerts and Client Notes	See general notes for the client and any alerts (Depending on access level)	X	X	X	X	X
Files	See files/documents associated to the client (Depending on access level)		X	X	X	X
Household Management	Manage members of the household	X	X	X	X	X
Location	Add and see history of locations of the client (Depending on access level)	X	X	X	X	X
Assessments	Add and see history of assessments of the client (Depending on access level)	X	X	X	X	X
Referrals	Refer clients to a program for services		X	X	X	X
Access Level	Description					
Attendance	For Swipe and Daily Attendance Tracking					X
Manage Agency	Managing program setups, program sites, staff usernames, etc.					X
Report Library	Library of reports available through Clarity (including HUD-required and LAHSA custom)		X	X	X	X
Analysis	Data Analysis Tool through Looker			X	X	X

Agency Sensitive Data	Access to sensitive data, including SSN.		X	X	X	X
Any Agency Sensitive Data	Access to sensitive data, including SSN that was entered by any agency.				X	X
Client Reports	Client-specific Reports such as ID Card for Printing, History, Notes, Summary		X	X	X	X
Caseload	List of clients associated to the user's account.		X	X	X	X
Attendance Standalone Module	For Swipe (TBD)					X
Aggregate Data Analysis	Data Analysis Tool through Looker			X		X
Referral Match Maker	Matching Functions				X	X
Restore Deleted Data	Restore Deleted Client Information			X		X
Navigator	Assigning					X
Data Import	Data Import Tool					X
Create New Clients	Create new client records		X	X	X	X
Create Service Placements	Record new services onto a client's record		X	X	X	X
Create Program Placements	Record new enrollments into a program onto a client's record		X	X	X	X
Create Public Alerts and Client Notes	Create notes and alerts on a client's record		X	X	X	X
Create Files	Add new files (scanned files, documents, etc.) onto a client's record		X	X	X	X

Create Location	Record a location for a client (whether for outreach, for permanent housing placements, etc.)		X	X	X	X
Create Assessments	Record a new assessment onto a client's record (Coordinated Assessment, Screening Tools, etc.)		X	X	X	X
Create Referral	Refer a client to a program		X	X	X	X
Edit Agency Services	Edit a service that was previously recorded by the user's organization on a client's record		X	X	X	X
Edit Any Agency Services	Edit a service that was previously recorded by any organization on a client's record					X
Edit Agency Program	Edit program enrollment information that was previously recorded by the user's organization on a client's record		X	X	X	X
Edit Any Agency Programs	Edit program enrollment information that was previously recorded by any organization on a client's record				X	X
Edit Agency Public Alerts and Client Notes	Edit a note or alert that was previously recorded by the user's organization on a client's record		X	X	X	X
Edit Any Agency Public Alerts and Client Notes	Edit a note or alert that was previously recorded by any organization on a client's record		X	X	X	X
Edit Agency Files	Edit files (scanned files, documents, etc.) that was previously uploaded by the user's organization on a client's record		X	X	X	X
Edit Any Agency Files	Edit files (scanned files, documents, etc.) that was previously recorded by any organization on a client's record				X	X
Edit Agency Location	Edit location information for a client that was previously recorded by the user's organization on a client's record		X	X	X	X
Edit Any Agency Location	Edit location information for a client that was previously recorded by any organization on a client's record				X	X

Edit Agency Assessment	Edit an assessment that was previously recorded by the user's organization on a client's record		X	X	X	X
Edit Any Agency Assessment	Edit an assessment that was previously recorded by the user's organization on a client's record				X	X
Edit Agency Referral	Edit a referral that was previously recorded by the user's organization on a client's record		X	X	X	X
Edit Any Agency Referral	Edit a referral that was previously recorded by any organization on a client's record				X	X
Delete Agency Services	Delete a service that was previously recorded by the user's organization on a client's record		X	X	X	X
Delete Any Agency Services	Delete a service that was previously recorded by any organization on a client's record					X
Delete Agency Programs	Delete program enrollment information that was previously recorded by the user's organization on a client's record		X	X	X	X
Delete Any Agency Programs	Delete program enrollment information that was previously recorded by any organization on a client's record					X
Delete Agency Public Alerts and Client Notes	Delete a note or alert that was previously recorded by the user's organization on a client's record		X	X	X	X
Delete Any Agency Public Alerts and Client Notes	Delete a note or alert that was previously recorded by any organization on a client's record					X
Delete Agency Files	Delete files (scanned files, documents, etc.) that was previously uploaded by the user's organization on a client's record		X	X	X	X
Delete Any Agency Files	Delete files (scanned files, documents, etc.) that was previously recorded by any organization on a client's record					X

Delete Location	Delete location information for a client that was previously recorded by the user's organization on a client's record		X	X	X	X
Delete Any Agency Location	Delete location information for a client that was previously recorded by any organization on a client's record					X
Delete Agency Assessment	Delete an assessment that was previously recorded by the user's organization on a client's record		X	X	X	X
Delete Any Agency Assessment	Delete an assessment that was previously recorded by the user's organization on a client's record					X
Delete Any Client	Delete any client records					X
Delete Agency Referral	Delete a referral that was previously recorded by the user's organization on a client's record		X	X	X	X
Delete Any Agency Referral	Delete a referral that was previously recorded by any organization on a client's record					X
<i>Last Revision By: Pada Lee</i>						
<i>Last Revision on: 4/21/2017</i>						

Appendix I: HMIS Access Policy

LA HMIS Implementation HMIS Access Policy

This policy describes how the Los Angeles County implementation of HMIS (LA HMIS) will approve access to HMIS.

Introduction

The [Homeless Emergency Assistance and Rapid Transition to Housing \(HEARTH\) Act of 2009](#) was signed into law on May 20, 2009 and amends and reauthorizes the McKinney-Vento Homeless Assistance Act to consolidate three separate homeless assistance programs administered by HUD into a single program – the Continuum of Care (CoC) Program. The [CoC Program Interim Rule](#), which guides the CoC Program and became effective August 30, 2012, with updates published on April 1, 2017, requires CoCs to designate a single Homeless Management Information System (HMIS) for the geographic area. The HMIS must comply with the Department of Housing and Urban Development's (HUD's) baseline requirements, as outlined in the [2004 HMIS Data and Technical Standards Final Notice](#) (Notice).

The HMIS Access Policy aims to ensure the confidentiality and security of all client data captured in the HMIS and conform with all current privacy and data confidentiality rights and regulations. The security and confidentiality of the personal information about people experiencing homelessness in an HMIS is a major consideration. For certain providers and sub-populations, such as Victim Services Providers (VSPs), HOPWA-funded shelters and programs, and substance abuse facilities, the security and confidentiality of client information becomes an even more significant concern. As a result, LA HMIS has implemented extensive technical and procedural measures to protect the confidentiality of personal information while allowing for reasonable, responsible, and limited uses and disclosure of data.

HUD Privacy & Security Standards

The Notice, published July 30, 2004, includes extensive HMIS privacy and security standards to be followed by CoCs, homeless assistance providers, and HMIS software companies. These standards were developed after carefully reviewing the Health Insurance Portability and Accountability Act (HIPAA) standards for securing protected health information. LA HMIS will implement and monitor practices and procedures to comply with the Privacy and Security Standards, as identified in the Notice and any subsequent updates to those standards.

Why do we use HMIS?

The HMIS database records and tracks client-level information about the characteristics and service needs of people at risk of and experiencing homelessness. LAHSA's HMIS solution ties together homeless service providers within a community to help create a more coordinated and adequate housing and service delivery system. Participating organizations and individual users within those organizations are granted access to HMIS based on their roles providing and coordinating services for people at-risk of and experiencing homelessness in Los Angeles County.

LA HMIS Access Criteria(s):

Access to HMIS is provided to relevant staff of **HMIS participating organizations**, which are organizations that operate within a CoC, provide services to individuals and households experiencing homelessness, and record, use, or process data for an HMIS. Prospective HMIS end users are provided access to HMIS in order to complete data collection related to federal and state-level funding, to participate in the coordination of services within the homeless system, and to assist the CoC in achieving its data-related goals.

In order to be eligible for access to HMIS, prospective HMIS end users must:

- Work for an HMIS participating organization as defined in Section 1.5 of the LA HMIS Policies and Procedures manual, which must be in good standing with the CoC for which they provide homeless services, and
- Provide or coordinate services to persons experiencing homelessness in Los Angeles County, **and**
- Have a business-related role (Direct Service, Administrative, or Technical/Data) requiring entry of or access to data in HMIS.

In accordance with the LA HMIS Policies and Procedures Manual, access to HMIS may only be provided to a prospective end user after execution of an End User Agreement between the user and HMIS Lead Agency and completion of required HMIS training. To maintain continued use of HMIS, end users must uphold the policies and procedures outlined in the LA HMIS Policies and Procedures Manual, including adhering to all privacy, security, and data quality plans of the respective CoC(s) for which they enter data.

In all cases outlined above, access will only be granted to individuals who interact with HMIS data in one of the following roles:

- **Direct Service Staff** are defined as those whose job description's note that their primary function is to connect with people experiencing homelessness, provide assessments of eligibility, and navigate to services including healthcare, public benefits, mental health and substance abuse treatment, shelter, and permanent housing and/or to coordinate the provision of these services. Staff with access are required to document in the HMIS system

services and coordination provided to participants. This also includes staff who directly supervise eligible direct service staff.

- **Administrative Staff** are defined as those who require access for payment or reimbursement for services.
- **Technical and/or Data Staff** are defined as those who require access to execute the functions of data management, data monitoring, quality assurance, data analysis, compliance, and/or an active data exchange initiative between HMIS and other related administrative data systems.

Special Considerations

The HMIS Lead Agency will request job descriptions or other written, supporting documentation to verify eligibility in cases where ambiguity exists.

Requests from Elected Offices: the HMIS Lead Agency will conduct an additional review procedure to deny or grant requests from any office of an elected governmental official, as outlined in the “HMIS Access Requests from Government Entities” process guide.

Requests from Law Enforcement Agencies: Law Enforcement Agencies and their employees are not eligible to participate in or access the LA County HMIS. The only allowable disclosures for law enforcement purposes must comply with and follow the procedures specified in 69 FR 45887 § 4.1.3 *Disclosures for law enforcement purposes (2004)*.

In all cases, and as stated in the End User Agreement, end users agree to maintain strict confidentiality of information obtained through HMIS, to use information obtained for or in HMIS only for the legitimate client service and administration of homeless projects provided by their organization. Any breach of client privacy or security will be sanctioned in accordance with the LA HMIS Policies and Procedures Manual, including possible termination of the end user’s participation in HMIS. Egregious violations of the LA HMIS access, privacy, or security policies may result in suspension of the HMIS participating organization’s access to HMIS. See **Security Violations and Sanctions** (below) for more information.

New Requests for Access:

New requests for access to LA HMIS must be made online through LAHSA's support portal:

1. Visit <https://lahsa.freshservice.com> and click Submit a Ticket.
2. Provide any relevant information to the request.
3. The request will be reviewed and responded to within two business days.
4. If LAHSA needs further information, you may be requested to:
 - a. Complete an implementation request form.
 - b. Join a scheduled call to discuss and provide the additional required information.

After all needed information has been provided, the request will go through an approval process consisting of HMIS Lead Agency staff and, depending on the CoC, others such as LHSA's Information Security team.

Anyone approved for access to the HMIS must first complete the following training and security prerequisites prior to receiving their user credentials:

- HMIS user training.
- All active HMIS users are required to complete the annual Security Awareness Training.
- All active users must participate in training on any updates to the system, policies, or procedures, as needed.
- All users must sign the Security Awareness Agreement, acknowledge receipt of a copy of the privacy notice, and pledge to comply with the privacy notice and additional terms and conditions for HMIS access.

The Approval Process:

New requests for access to HMIS will go through the following approval process:

1. LAHSA's HMIS Implementation Analyst will review the request to ensure it meets the minimum requirements based on the participating organization type and role.
2. Upon verification of access requirements:
 - a. Homeless Service Providers will be approved by the HMIS Implementation Analyst and move to the implementation process.
 - b. Any other entity type will be sent to LAHSA leadership for review and approval.
3. If approved, the request will be moved on to the implementation process. If denied, the entity will be provided with a reason for the denial and an appeal process (described below).

The Implementation Process:

Once approved for access to LA HMIS, the prospective end user will go through the following process:

1. The following forms must be signed and submitted to LAHSA:
 - a. HMIS Participating Organization Agreement
2. The entity will be provided with the following documents:
 - a. LA HMIS Policies and Procedures
 - b. LA HMIS Privacy Notice
3. The entity's agency profile and applicable programs will be set up in HMIS.

4. Anyone individual approved for access to the HMIS must first complete and maintain the following training and security prerequisites prior to receiving their HMIS end user credentials:
 - a. All active users are required to complete HMIS user training.
 - b. All active HMIS users are required to complete the annual Security Awareness Training.
 - c. All active users must participate in training on any updates to the system, policies, or procedures, as needed.
 - d. All users must sign the Security Awareness Agreement, acknowledge receipt of a copy of the privacy notice, and pledge to comply with the privacy notice and additional terms and conditions for HMIS access.
 - e. All users must acknowledge that they understand and agree to the HMIS Policies and Procedures.

Ongoing Monitoring of HMIS Users:

LAHSA's HMIS Implementation Analyst will monitor HMIS usage for all entities and users. To retain access to LAHSA's HMIS, each entity must:

- **Have enrollments, services, notes, or assessments entered each month for non-PH projects or each year for P.H. projects. This does not apply to entities with read-only access.**
 - **Projects not in use may be deactivated if no recent activity exists (or deleted if no clients have been entered since initial implementation).**
- **Maintain at least one active user each month. Users will be automatically deactivated after 30 days of inactivity. When a user account is disabled for inactivity, a user can get reactivated with no training requirements for up to 90 days. After 90 days of inactivity, a user will undergo HMIS re-training to get activated.**

Entities will receive an email notification within five business days before any adjustments are made to their programs or access levels.

All participating entities (Providers, Cities, County Agencies, and Healthcare Organizations) must notify LAHSA of the need to deactivate system users within 24 hours of termination.

Security Violations and Sanctions:

Any user violating security protocols of their agency's procedures or HMIS Access Policies and Procedures will be sanctioned accordingly. In addition, end users found in violation may be temporarily or permanently suspended from HMIS based on an investigation of the violations. LASHA's Risk Management will conduct all user violations of HMIS, which will be shared with the CoC Board.

If the end user’s violation involves the organization’s management/leadership, the HMIS Lead Agency may escalate its review to include the participating organization itself. HMIS participating organizations whose leadership has contributed to security violations may face additional sanctions from LA HMIS, including possible suspension of the organization’s access to HMIS depending on the severity of the violation(s).

The table below lists the progression of warnings and actions taken by the HMIS Lead Agency and the CoC in cases of security violations. The CoC reserves the right to immediately and permanently revoke access from a user or agency without the complete three warnings depending on the severity of the violation(s). A monthly report will be provided to the CoC Board on any violations of the HMIS Access Policy.

Warnings	Result
First Warning	The HMIS Lead Agency will inform the relevant CoC leadership of all violations, and the user will be notified in writing to ensure the offense doesn't happen again.
Second Warning	Temporary suspension from HMIS with mandatory refresher training ensures each end user understands the HMIS Security procedures and expectations.
Third Warning	After providing training, the user continues violating the HMIS Access Policy. Permanent suspension from HMIS access across the CoC will be enacted. The suspension cannot be appealed.

HMIS end user bans are specific to the user and will transfer across participating organizations. Any end user who has been banned from HMIS and subsequently submits for access will receive notification of denial, sent to both the user and the participating organization for which they are associated. This includes end users who were banned while associated with one participating organization and are re-applying under association with a different participating organization.

Additionally, individual users, participating organizations, and/or other entities found in violation of this policy may be referred to Los Angeles County's Fraud Hotline and/or law enforcement agencies for additional investigation and possible prosecution. The CoCs reserve the right to immediately make this referral without issuing three warnings, depending on the severity of the violation(s).

All HMIS users will follow the data release Policies and Procedures to guide the data release of client information stored in HMIS. For CA-600 end users, LAHSA Risk Management will investigate egregious violations.

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

No identifiable client data will be released to any person, agency, or organization for any purpose without written permission from the client.

User Appeals Processes:

The HMIS participating organization of any user who has been denied access to HMIS (either at initial request or due to security violation) may submit an appeal to the HMIS Lead Agency, detailing reasons why access should be granted or restored.

User Access Request Denials:

1. Appeals must be submitted in writing to the HMIS Lead Agency, detailing reasons why the prospective end user's access is in accordance with the HMIS Access Policy.
2. If the HMIS Lead Agency grants the appeal, the implementation process will proceed as described above.
3. If the HMIS Lead Agency upholds the initial denial, the appeal will be submitted to the next level of HMIS governance (generally, either an HMIS Committee or the CoC Board, depending on the CoC for which the end user is seeking access).
4. The appeal request will be added to the agenda of the committee or board's next scheduled meeting, and follow established governance procedures for consideration and voting.
5. Upon being notified of the vote's outcome, the HMIS Lead Agency will inform the participating agency within 2 business days.

User Security Violation-Related Suspensions:

1. Upon receipt of an appeal request from the suspended end user's participating organization, the HMIS Lead Agency will conduct an internal investigation. The end user's account will remain deactivated until the internal investigation has been completed.
2. Following the internal investigation, the HMIS Lead Agency will notify the end user's participating organization of any substantiated incidents that may have compromised HMIS system security or client privacy, whether or not a release of client PPI is definitively known to have occurred. If the security or privacy concern resulted from demonstrated noncompliance by an end user with the HMIS End User Agreement, the HMIS Lead Agency reserves the right to maintain permanent deactivation of the HMIS account of the end user in question.
3. Within 5 business days after the HMIS Lead Agency receives notice of the security or privacy concern, the HMIS Lead Agency and participating organization will jointly establish an action plan to analyze the source of the security or privacy concern and actively prevent

such future concerns. The action plan shall be implemented as soon as possible, and the total term of the plan must not exceed thirty (30) days.

4. If the participating agency is not able to meet the terms of the action plan within the time allotted, the HMIS Lead Agency, in consultation with the respective CoC's HMIS advisory board (HMIS Committee, CoC Board, etc.), may elect to terminate the end user's access to HMIS. The participating agency may appeal to the HMIS Lead Agency for reinstatement to HMIS following completion of the requirements of the action plan.

Participating Organization Appeals Process:

An HMIS participating organization that has been denied access to HMIS due to security violation(s) may submit an appeal to the HMIS Lead Agency, detailing reasons why access should be restored.

Agency Security Violation-Related Suspensions:

1. Upon receipt of an appeal request from the suspended participating organization, the HMIS Lead Agency will conduct an internal investigation. The organization will remain deactivated until the internal investigation has been completed.
2. Following the internal investigation, the HMIS Lead Agency will notify the participating organization of any substantiated incidents that may have compromised HMIS system security or client privacy, whether or not a release of client PPI is definitively known to have occurred.
3. Within 5 business days after the HMIS Lead Agency receives notice of the security or privacy concern, the HMIS Lead Agency and participating organization will jointly establish an action plan to analyze the source of the security or privacy concern and actively prevent such future concerns. The action plan shall be implemented as soon as possible, and the total term of the plan must not exceed thirty (30) days.
4. If the participating organization is not able to meet the terms of the action plan within the time allotted, the HMIS Lead Agency, in consultation with the respective CoC's HMIS advisory board (HMIS Committee, CoC Board, etc.), may elect to terminate the organization's access to HMIS. The participating organization may appeal to the HMIS Lead Agency for reinstatement to HMIS following completion of the requirements of the action plan.
5. Organizations that have been terminated from HMIS and unsuccessfully appealed that sanction may re-apply for access to HMIS after a suspension term of one year.