Homeless Management Information System (HMIS) Policies and Procedures

Los Angeles/Orange County HMIS Collaborative

Continuum Of Care Lead Entities:
City Of Glendale
City Of Pasadena
Los Angeles Homeless Services Authority
Orange County

Last updated on: 10/29/2015

HMIS LEAD AGENCIES CONTACT INFORMATION

City of Glendale

City of Glendale has its own Continuum of Care

141 North Glendale Avenue, Glendale, CA 91206

Tel: (818) 548-3720
Fax: (818) 548-3724

HMIS Contact Information		
Team	**Contact Email**	**Reason**
HMIS Program Assistant	isamvelyan@ci.glendale.ca.us	Requests for support related to data quality and management.
HMIS Administrator	isamvelyan@ci.glendale.ca.us	▪ General technical support for HMIS issues related to user access, troubleshooting, information requests, system functionality errors, etc. ▪ Training ▪ Requests for issues related to data quality, management and/or mandated reports, report failure, etc. ▪ Requests for issues related mandated reports, report failure, etc.

City of Pasadena

City of Pasadena has its own Continuum of Care

649 North Fair Oaks Avenue, Pasadena, CA 91103

Tel: (626) 744 - 6701
Fax: (626) 744 - 8340

HMIS Contact Information		
Team	**Contact Email**	**Reason**
HMIS Program Assistant	alansing@CityofPasadena.net	Requests for support related to data quality and management.
HMIS Administrator	onazarian@CityofPasadena.net	▪ General technical support for HMIS issues related to user access, troubleshooting, information requests, system functionality errors, etc. ▪ Training ▪ Requests for issues related to data quality, management and/or mandated reports, report failure, etc. ▪ Requests for issues related mandated reports, report failure, etc.

Los Angeles Homeless Services Authority (LAHSA)

LAHSA is the lead entity responsible for the Los Angeles Continuum of Care comprised of the County of Los Angeles except for the cities of Pasadena, Glendale, and Long Beach which have their own Continuum.

811 Wilshire Boulevard, Los Angeles, CA 90017

Tel: (213) 683-3333
Fax: (213) 892-0093
TTY: (213) 553-8434

HMIS Contact Information		
Team	**Contact Email**	**Reason**
HMIS Support	HMISSupport@lahsa.org	General technical support for HMIS matters related to user access, troubleshooting, information requests, system functionality errors, etc.
HMIS Training	HMISTraining@lahsa.org	Training
IT Hardware Support	ITSupport@lahsa.org	General technical support for hardware failures, connectivity issues, etc.
Data Analysts	DataAnalysts@lahsa.org	Requests for support related to data quality, management and/or mandated reports, report failure, etc.

LAHSA HMIS Website
http://hmis.lahsa.org/

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

LAHSA HMIS Version 5.5
http://lahsahmis.esserver.com/

Last updated on: 10/29/2015

Orange County

Orange County has its own Continuum of Care.

1505 East 17th Street, Suite 108, Santa Ana, CA 92705

Tel: (714) 589-2360
Fax: (714) 258-7852

HMIS Contact Information		
Team	**Contact Email**	**Reason**
HMIS Assistance and Training	HMIS-helpdesk@211oc.org	▪ General technical support for HMIS issues related to user access, troubleshooting, information requests, system functionality errors, etc. ▪ Training ▪ Requests for issues related to data quality, management and/or mandated reports, report failure, etc.

OC HMIS Website
http://ochmis.org/

OC HMIS Training Website
http://ochmis.org/hmis-help/

OC HMIS Version 5.5
http://ochmis.esserver.com/

PROJECT SUMMARY

Background

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

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

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

In 2010 the U.S. Interagency Council on Homelessness (USICH) affirmed HMIS as the official method of measuring outcomes in its Opening Doors: Federal Strategic Plan to Prevent and End Homelessness. Since then many of the federal agencies that provide McKinney-Vento Act and other sources of funding for services to specific homeless populations have joined together and are working with HUD to coordinate the effort.

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

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

Programs that receive other sources of funding are not required to participate in the HMIS, but are strongly encouraged to do so to contribute to a better understanding of homelessness.

The HMIS Data Standards (published in the 2014 HMIS Data Dictionary and HMIS Data Manual) provide communities with baseline data collection requirements developed by each of these federal partners.

LA/OC HMIS is a response to the HUD mandated implementation of a Homeless Management Information System (HMIS) database. The LA/OC HMIS is an online database used by homeless and at-risk service providers that records demographic and service usage data and produces an unduplicated count of the people using those services.

The LA/OC HMIS implementation is led by the LA/OC HMIS Collaborative.

LA/OC HMIS Collaborative

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

- In Los Angeles County, there are three CoCs: (1) City of Glendale, (2) City of Pasadena, and the (3) Los Angeles Homeless Services Authority (LAHSA) responsible for the City of Los Angeles and the balance of Los Angeles County.

- People for Irvine Community Health dba 211 Orange County and its partner Orange County Community Services coordinate the Orange County CoC.

The LA/OC Collaborative brings the following advantages:

- Comprehensive, consistent and coordinated provision of services to homeless persons between CoCs to meet the specific needs of the homeless persons.
- Enhanced understanding of homeless needs, service usage, effectiveness and gap through the use of regional data and reports to make informed decisions.

Mission Statement

The LA/OC HMIS Collaborative will use the LA/OC HMIS to advance the provision of quality services for homeless and at risk homeless persons, improve data collection and promote more responsive policies to prevent and end homelessness in the Los Angeles County and Orange Counties.

Vision

The LA/OC HMIS Collaborative is dedicated to providing the best possible, highest quality regional HMIS to enhance the delivery of services for persons who are homeless or at risk of homelessness. Specifically, the LA/OC HMIS will:

- Facilitate the coordination of service delivery for homeless and at risk homeless persons.

- Enable agencies to track referrals and services provided, report outcomes, and manage client data using an accessible, user-friendly and secured technology.
- Enhance the ability of policy makers and advocates to gauge the extent of homelessness and plan services appropriately throughout Los Angeles and Orange Counties.

LA/OC HMIS Software

LA/OC HMIS is a comprehensive case management system that allows the LA/OC Collaborative and Users to use the collected information to make informed program decisions. It also includes a focus on outcomes management intended to provide value by allowing the user to set and measure client and program milestones and target achievements.

LA/OC HMIS includes the following components:

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

1. ROLES AND RESPONSIBILITIES

1.1 LA/OC HMIS Collaborative Responsibilities

Policy:

The Collaborative will be responsible for the organization and management of the LA/OC HMIS.

Responsibilities:

The Collaborative is responsible for all system-wide policies, procedures, communication, and coordination. It is also the primary contact with Adsystech, and with its help, will implement all necessary system-wide changes and updates.

Procedure:

- HMIS Administrators are the primary positions at the LA/OC Collaborative for HMIS management.

1.2 HMIS Administrator Responsibilities

Policy:

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

Responsibilities:

The HMIS Administrator is responsible for:

- Providing training support to Participating Organization by determining training needs of Users, developing training materials, and training Users in equipment and software;
- Providing technical support by troubleshooting data with Participating Organization;
- Managing user accounts and access control;
- Identifying and developing system enhancements and communicating to Participating Organization of these changes;
- Communicating system-related information to Participating Organization.
- Developing and modifying reports for Users based on requests.

Procedure:

- Each CoC will have a designated HMIS Administrator(s).

1.3 Organization Administrator Responsibilities

Policy:

Each Participating Organization must designate an Organization Administrator and a backup Organization Administrator responsible for the oversight of all personnel that generate or have access to client data in the LA/OC HMIS to ensure adherence to the Policies & Procedures described in this document.

Responsibilities:

The Organization Administrator is responsible for:

- Serving as the primary contact between Users and HMIS Administrator;
- Providing technical support by troubleshooting data 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 to User if applicable to the local organization's region;
- Notifying the HMIS Administrator of personnel changes;
- 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 and adherence and understanding of the HMIS User Agreement;
- Ensuring organizational adherence to the Policies and Procedures;
- Detecting and responding to violations of the Policies and Procedures.

Procedure:

- Participating Organization must provide their local HMIS Lead Agency the name and contact information of the Organization Administrator and backup Organization Administrator.
- Any changes to that information must be reported to the HMIS Administrator.

1.4 HMIS Lead Agency Communication with Participating Organization

Policy:

The HMIS Administrator is responsible to communicate any system-related information to participating organizations in a timely manner.

Procedure:

- HMIS Administrators will send email communication to the Organization Administrator.
- Organization Administrators are responsible for distributing information and ensuring that all members of their organization are informed of appropriate HMIS related communication.
- Specific communications will be addressed to the person or parties involved.

- Each HMIS Lead Agency will also distribute HMIS information on their designated website.

1.5 Participating Organization Communication with HMIS Lead Agency

Policy:

The Participating Organization is responsible for communicating needs and questions regarding the LA/OC HMIS to the HMIS Administrator a timely manner.

Procedure:

- Participating Organization will send email communication to the HMIS Administrator.
- Specific communications will be addressed to the person or parties involved.

2. IMPLEMENTATION POLICIES AND PROCEDURES

2.1 HMIS Organization Agreement Requirement

Policy:

The Executive Director of any Participating Organization shall follow, comply, and enforce the HMIS Organization Agreement (Appendix A). The Executive Director must sign the HMIS Participating Organization Agreement before granted access to the LA/OC HMIS.

Procedure:

- An original signed HMIS Participating Organization Agreement must be presented to the HMIS Administrator before any program is implemented in the LA/OC HMIS.
- After HMIS Participating Organization Agreement is signed, the HMIS Administrator will train Users to use the LA/OC HMIS.
- A username and password will be granted to Users after required training is completed.
- Signing of the HMIS Participating Organization Agreement is a precursor to training and user access.

2.2 HMIS User Agreement Requirement

Policy:

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

Procedure:

- The HMIS Administrator will provide the User a HMIS User Agreement for signature after required training is completed.
- The HMIS Administrator will collect and maintain HMIS User Agreements of all Users.

2.3 Data Collection Requirements

Policy:

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

Procedure:

- Participating Organization 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 HMIS Data Standards Manual released May 2014.

  The universal data elements include:

  - Name
  - Social Security Number
  - Date of Birth
  - Race
  - Ethnicity
  - Gender
  - Veteran Status
  - Disabling Condition
  - Residence Prior to Project Entry
  - Project Entry Date
  - Project Exit Date
  - Destination
  - Personal ID
  - Household ID
  - Relationship to Head of Household
  - Client Location
  - Length of Time on Street, in and ES or Safe Haven

- Users must also collect all the program-specific data elements at project entry and exit set forth in the HMIS Data Standards released May 2014. The program-specific data elements include:

  - Housing Status
  - Income and Sources
  - Non-Cash Benefits
  - Health Insurance
  - Physical Disability
  - Chronic Health Condition
  - HIV/AIDS
  - Mental Health Problem
  - Substance Abuse
  - Domestic Violence
  - Contact
  - Date of Engagement
  - Services Provided
  - Financial Assistance Provided
  - Residential Move-in Date
  - Housing Assessment Disposition
  - Housing Assessment At Exit

- These standards are already required fields in the LA/OC HMIS. For other funder specific program data elements refer to the 2014 Data Standards Manual.

2.4 Technical and Security Standards

Policy:
Participating Organization must meet the technical standards outlined below to participate in the LA/OC HMIS.

Minimal Hardware Requirements	
Components	**Requirement**
Windows	X86 or X64 1.6-gigahertz (GHz) or higher processor 1 GB of RAM
	1 GB of Memory & 10 GB Free Disk Space
	10/100 Network Interface Card
	1280 by 800 pixels Screen Resolution
Macintosh (Intel-based)	Intel Core Duo 1.83-gigahertz (GHz) or higher processor with 1 GB of RAM
	1 GB of Memory & 10 GB Free Disk Space
	1280 by 800 pixels Screen Resolution

Minimal Bandwidth Requirements	
Required	**Preferred**
128 kbps Upload Speed	1.5 Mbps Upload Speed
768 kbps Download Speed	3 Mbps Download Speed
75% Quality of Service	90% Quality of Service

Compatible Operating Systems and Browsers					
Operating Systems	**IE 9**	**IE 8**	**IE 7**	**Firefox 4+**	
Windows 8					
Windows 7	X	X		X	
Windows Vista					
Macintosh OS 10.4.11+ (Intel based)				X	

Minimal Microsoft Requirements	
Windows	**Mac**
	MS Silverlight 4.0
	Silverlight must be installed on the computer before using HMIS, please visit Silverlight Installation website: http://www.microsoft.com/getsilverlight
MS Silverlight 4.0	

- Connection to the internet is the sole responsibility of the Participating Organization and is a requirement to participate in the LA/OC HMIS.
- All Operating systems should have the latest Service Pack 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 definition must be updated regularly.

2.5 Maintenance of Onsite Computer Equipment

Policy:

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

Procedure:

- The Executive Director (or other empowered officer) will be responsible for the maintenance and disposal of onsite computer equipment. This includes:
    - Purchase of and upgrades to all existing and new computer equipment for utilization in the system.
    - Workstations accessing the system must have a username/password to log onto Microsoft Windows Operating System.
    - Workstation accessing 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:

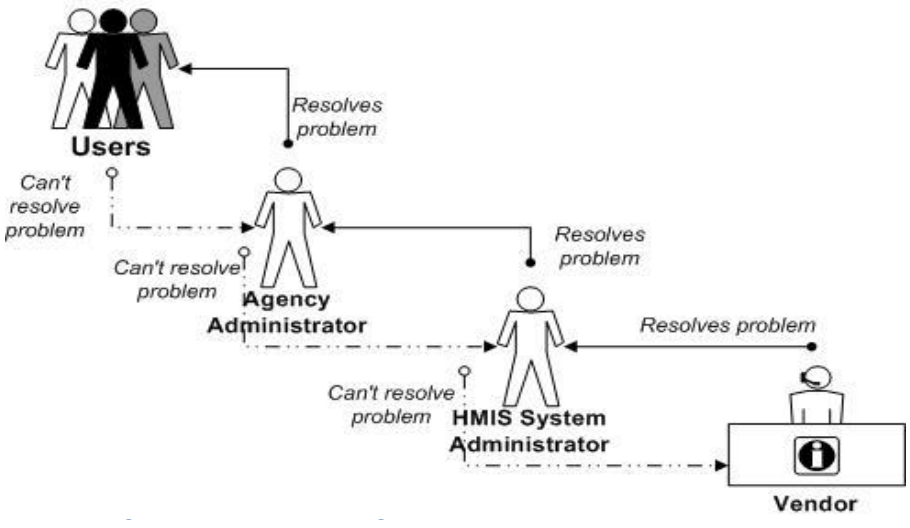
Each HMIS Lead Agency will provide technical support to all Participating Organization as needed.

Procedure:

1. Users should first seek technical support from the Organization Administrator.
2. If more expertise is required to further troubleshoot the issue, Organization Administrator will contact the HMIS Administrator (See Technical Assistance Flow Chart).
3. Technical support Hours are Monday through Friday (excluding holidays) from 9:00 am to 5:00 pm.
4. The Organization Administrator will provide issue details if possible (or help recreate the problem by providing all information, screenshots, reports, etc.) in order for the HMIS Administrator to recreate the problem.
5. 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 affect response time.
6. The HMIS Administrator will submit a ticket to vendor if progress is stalled.

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

Technical Assistance Flow Chart



Policy:

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

Procedure:

- The vendor will communicate to the Collaborative Lead Member and backup of any necessary downtime for system upgrades and patches. These will be performed in the late hours when possible.
- In the event that it is determined that the LA/OC HMIS accessibility is disabled system-wide, the HMIS Administrators will analyze and determine the problem.
- The HMIS Administrator will work with the software vendor to repair the problem.
- The HMIS Administrators will send email communication to the Organization Administrator within 2 hours of problem awareness and informed them of estimated system availability.

2.7 Participation Fees

Policy:

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

Procedure:

- Consult local HMIS Lead Agency regarding fees.

3. SECURITY POLICIES AND PROCEDURES

3.1 User Authentication

Policy:

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

Procedure:

- The Participating Organization will determine which of their employees will have access to the LA/OC HMIS. User access will be granted only to those individuals whose job functions require legitimate access to the system.
- Proposed User must complete the required training and demonstrate proficiency in use of system.
- Proposed User must sign the HMIS User Agreement stating that he or she has received training, will abide by the 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 receipts of these Policies and Procedures.
- The HMIS Administrator will assign new user with a username and an initial password.
- Sharing of usernames and passwords will be considered a breach of the HMIS User Agreement since it compromises the security to clients.
- Organization Administrator is required to notify the HMIS Administrator when User leaves employment with the organization or no longer needs access.
- HMIS Administrator will terminate access upon notification of the Organization Administrator within 1 week of receiving the Revocation Form.

3.2 Passwords

Policy:

User will have access to the LA/OC HMIS via a username and password. Passwords will be reset every 180 days. User will maintain passwords confidential.

Procedure:

- The HMIS Administrator will provide new User a unique username and temporary password after required training is completed.
- User will be required to create a permanent password that is between eight and sixteen characters in length. It must also contain characters from the following four categories: (1) uppercase characters (A through Z), (2) lower case characters (a through z), (3) numbers (0 through 9), and (4) non-alphabetic characters (for example, $, #, %).

- 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, but may use the same password more than once.
- After 10 minutes of inactivity, User will get a session timeout warning popup that will allow users to continue their session or will automatically log the user off after 10 minutes of inactivity.
- User ability to reset own password from 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 password is reset by the HMIS Administrator. The Organization Administrators will need to contact the HMIS Administrator to regain access.

3.3 Extracted Data

Policy:

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

3.4 Encryption Management

Policy:

Client data stored on the central server will always be encrypted except during specific procedures.

Procedure:

- Client data will only be decrypted when the LA/OC HMIS server becomes obsolete and necessitates an upgrade in technology. Should the necessity arise, the HMIS Administrator, on behalf of the vendor, will obtain the written permission of the Executive Management of each Participating Organization to perform the decryption and subsequent database conversion to a new technology.

3.5 Hardware Security Measures

Policy:

All computers and networks used to access LA/OC 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 Organization has virus protection software and firewall installed prior to granting LA/OC HMIS access.
- Virus definition must be updated regularly.
- Firewall must be placed between any computer and internet connection for the entire network, be protected with at minimum Wired Equivalent Privacy (WEP), use Network Address Translation (NAT), and maintain the most recent virus security updates.
- The Organization Administrator will ensure that computers maintain security specifications.

3.6 Backup and Recovery Procedures

Policy:

The 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/OC HMIS.

Procedure:

- The 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 vendor.

- The vendor shall maintain an off-site storage of tapes in fire proof containers.

- The 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/OC 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.

3.7 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 Organization.

Procedure:

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

3.8 Security Violations and Sanctions

Policy:

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

Procedure:

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

4. OPERATIONAL POLICIES AND PROCEDURES

4.1 User Access Levels

Policy:

User will be designated a user access level that controls the level and type of access the user has within the LA/OC 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.
- The table below lists the levels of access tied to existing user roles across the LA/OC Collaborative. This might include a role not available within local continuum. Consult local HMIS Lead Agency to learn which user access levels are available, as well as other customizable roles, such as Coordinated Entry, that may be offered in consultation and with approval from the HMIS Administrator (See HMIS Lead Agencies Contact Information).

User Role	Level of Access	Description
HMIS Administrator	Access to all libraries and pages within the LA/OC HMIS.	This role will grant access to system-wide data in order to support all participating organizations, meet reporting requests, and other system administration responsibilities.
Organization Administrator	Access to Central Intake, Agency Services, and other system libraries.	This role will grant access to data collected by their own organization.
Case Manager	Access to Central Intake and Agency Services libraries.	This role will grant access to data collected by their own organization.
Outreach	Access to Central Intake, Agency Services, and Outreach libraries.	This role will grant access to data collected by their own organization.
Report	Access only to Management and/or Ad-hoc Reports.	This role will only allow generating reports. Cannot enter and/or modify client data.

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/OC 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, if applicable for the local organization's region. 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.
- The table below lists the training courses offered across the LA/OC Collaborative. This might include a course not available within local continuum. Please consult local HMIS Lead Agency to learn about available training courses.
- For LAHSA Participating Organization, see the Supplemental Policies for LAHSA Only: LAHSA Training Requirements.

Course Description	Course Detail	Required
HMIS Basic User Training	This course focuses on Policies and Procedures, review of HUD Data and Technical Standards, Privacy and Mandatory Collection Notices and consents. Also, on the navigation of the LA/OC HMIS.	All new Users.
Ethics and Confidentiality Training	This course focuses on ethics and confidentiality.	All new Users.
Security Training	*This will be a new course based on the upcoming Federal Regulations.	All new and existing Users.
Organization Administrator Training		Agency Administrators
Reporting Training	This course focuses on management reports.	

4.3 User Guide

Policy:

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

Procedure:

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

HIPAA-Covered Entities:

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

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

4.5 Revocation of Consent

Policy:

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

Procedure:

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

4.6 Data Sharing

Policy:

Client data (with consent) contained in Central Intake Library will be shared with other Participating Organization. Sharing of program level client data between Participating Organization will require a signed Interagency Sharing Agreement and/or Consent to Share Protected Personal Information.

Procedure:

- Data sharing refers to the sharing of information between Participating Organization for the coordination of case management and client service delivery.
- Sharing of program level client data between Participating Organization will require a signed Interagency Sharing Agreement (Appendix G).
- Participating Organization must store signed Interagency Sharing Agreement in client record for auditing purposes.
- Users found to be sharing program level client data without consent will have their access terminated.

4.7 Client Record Access

Policy:

Client may inspect and obtain 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 Central Intake Library can be provided at any organization the client requests it from, as long as 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 Central Intake Library.
- The Organization Administrator will review client information with client if he or she requests to view their HMIS data.
- No client shall have access to another client record in the system.
- 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.
- Parental or guardian access will be decided based upon existing organization guidelines.

4.8 Client Grievance

Policy:

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

Policy:

All data entered into the LA/OC HMIS must meet data quality standards. Users will be responsible for the quality of their data entry.

- ### Definition:

  Data quality refers to the timeliness, completeness, and accuracy of information collected and reported in the LA/OC HMIS.

Data Timeliness:

Users must enter all universal data elements and program-specific data elements within 3 days of intake.

Data Completeness:

All data entered into the system is complete.

Data Accuracy:

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

Procedure:

- Participating Organization 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 Organization will collect and enter as much relevant client data as possible for the purposes of providing services to that client.
- All data will be input into the system no more than 3 days of program entry.
- The HMIS Administrator will conduct random 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 monitor 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/OC HMIS.

Definitions:

Client data may be used or discloses for system administration, technical support, program compliance, analytical use, and other purposes as required by law. 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 Organization may use data contained in the system to support the delivery of services to homeless clients in the Los Angeles and Orange Counties. Organizations may use or disclose client information internally for administrative functions, technical support, and management purposes. Participating Organization may also use client information for internal analysis, such as analyzing client outcomes to evaluate program.
- Each of the continuums within the LA/OC HMIS Collaborative shall have access to their respective agencies' client data stored in the system. The Collaborative will use the data for the purposes for administrative functions, technical support, program compliance, and analytical use. The Collaborative will not disclose personal identifiable client data.
- The vendor and any authorized subcontractor shall not use or disclose data stored in the LA/OC HMIS without expressed written permission in order to enforce information security protocols. If granted permission, the data will only be used in the context of interpreting data for research and system troubleshooting purposes. The Service and License Agreement signed individually by each Continuum and vendor contain language that prohibits access to the data stored in the software except under the conditions noted above.

5.3 Data Release

Policy:

All LA/OC HMIS stakeholders will follow the data release Policies and Procedures to guide the data release of client information stored in the LA/OC 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 to any person, agency, or organization for any purpose without written permission from the client.
- Each Participating Organization owns all data that is stored in the system. The organization may not release personal identifiable client data without written permission from the client. Organizations may release program and/or aggregate level data for all clients to whom the organization provided services. No personal identifiable client data will be provided to any group or individual that is neither the Participating Organization that entered the data without written consent by the client.
- Each of the continuums within the LA/OC HMIS Collaborative may release aggregate data about its own continuum at the program, sub-regional, and regional level. Aggregate data may be released without organization permission at the discretion of the Continuum. It may not release any personal identifiable client data to any group or individual. The Collaborative may develop an annual release of aggregate data in a summary report format.

5.4 Data Migration

Policy:

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

Definition:

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

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

Procedure:

- Migrated data must be non-duplicated and an exact match to the existing field type of the LA/OC HMIS. The Participating Organization will be responsible for the accuracy, completeness, and quality of the migrated data.
- The existing system of the Participating Organization must be an ODBC-compliant database platform in order for migration to be possible. The HMIS Administrator can help the organization determine the ODBC compatibility for any legacy systems.
- Only data that is an exact match with LA/OC HMIS data fields may be migrated. Data must be unduplicated prior to data migration. All required fields in the LA/OC HMIS are required for migration. A data dictionary will be provided upon request.
- The HMIS Administrator will decide the appropriate data migration candidates. If approved, a Transfer of Data Agreement must be completed and the Organization will provide current data in an ODBC usable form 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/OC HMIS.
- All costs associated with the Transfer of Data will be at the expense of the organization.

6. TERMINOLOGY

Adsystech: Software developer of the Adaptive Enterprise Solutions© technology for the LA/OC HMIS.

Organization Administrator: The person responsible for system administration at the organization level. Responsibilities include informing HMIS System Administration of the need to add and delete users, basic trouble-shooting, and escalation of issues to their HMIS Administrator. This person is the organization user's first line of contact for LA/OC HMIS issues.

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

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

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

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

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

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

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

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

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

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 plan text via decryption.

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

HMIS: Homeless Management Information System. This is a generic term for any System used to manage data about the use of homeless services.

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

HMIS User: An individual who has unique user identification (ID) and directly accesses the LA/OC 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 at the system or aggregate level or organization users that perform functions at the organization level.

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

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

Network: Several computers connected to each other.

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

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

7. APPENDICES

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

Appendix A: HMIS Participating Organization Agreement

GREATER LOS ANGELES & ORANGE COUNTY
HOMELESS MANAGEMENT INFORMATION SYSTEM (LA/OC HMIS)

PARTICIPATING ORGANIZATION AGREEMENT

I. Purpose

The HMIS is a HUD-mandated information technology system that is designed to capture client-level information over time, on the characteristics and service needs of homeless persons. Client data is maintained on a central server, which will contain all client information in an encrypted state. HMIS integrates data from all homeless service providers and organizations in the community and captures basic descriptive information on every person served. Participation in LA/OC HMIS allows organizations to share information with other participating organizations to create a more coordinated and effective delivery system.

The LA/OC HMIS is the secured electronic database for the Greater Los Angeles and Orange Counties and is a valuable resource for local communities. The LA/OC HMIS Collaborative consists of four separate Continuums of Care (CoC). The continuums are: Los Angeles City and County; Santa Ana/Anaheim/Orange County; Glendale; and Pasadena.

The LA/OC HMIS Collaborative's goal is to provide a comprehensive case management system to advance the provision of quality services for homeless persons, improve data collection, and promote more responsive policies to end homelessness in the Greater Los Angeles and Orange Counties.

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/OC HMIS, on behalf of this Organization. In order to allow a User to access the LA/OC 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/OC 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 entered into 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 entered into the LA/OC HMIS must sign the *Consent to Share Protected Personal Information* form.

Verbal Consent: Verbal consent to enter PPI into the LA/OC HMIS may be obtained during circumstances such as phone screenings, street outreach, or community access center sign-ins. Each client must be informed that his or her information will be entered into 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 his or her 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 his or her consent form
- A copy of his or her HMIS records
- A current list of participating organizations that have access to HMIS data

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/OC HMIS is not accessible to unauthorized users
- LA/OC HMIS is only accessed by computers approved by the Organization
- HMIS Users are trained regarding user responsibilities and conduct
- HMIS Users sign and comply with the *LA/OC HMIS User Agreement*

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

> ***Equipment, if applicable****:* All CoC-provided computer equipment including, but not limited to, printers, scanners, laptops and monitors, were provided through grant funds from HUD. The maintenance and upgrades of these devices are subject to the requirements and funding limitations of the HUD grant. Maintenance and/or upgrade costs to equipment, incurred after the HUD grant funds have been exhausted, become the sole responsibility of this Organization.
>
> ***Software, Licenses, and/or Services, if applicable****:* CoC-provided services to each organization may include, but are not limited to, purchasing and installing Anti-Virus Software and licenses, Firewall software and licenses, Windows software updates and High-Speed Internet Connections. The software and/or services are provided for HMIS purposes through HUD grant funds. The maintenance, upgrades and license purchases are subject to the requirements and funding limitations of the HUD grant. Additional maintenance, upgrades and license purchases, incurred after the grant funds have been exhausted, become the sole responsibility of this Organization.

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

IX . Copyright
The LA/OC 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/OC CoC reserves the right to amend this agreement by providing a 3-day notice to this Organization.
- Either party has the right to terminate this agreement, with or without cause, by providing a 3-day written notice to the other party.
- If this agreement is terminated, this Organization shall no longer have access to HMIS or any information therein. The remaining LA/OC 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/OC HMIS agree to abide by LA/OC's 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 Organization. Upon final execution, this Organization will be given access to the LA/OC 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 & ORANGE COUNTY
HOMELESS MANAGEMENT INFORMATION SYSTEM (LA/OC HMIS)

USER AGREEMENT

I. Purpose

The LA/OC HMIS is the secured electronic database for the Greater Los Angeles and Orange Counties and is a valuable resource for local communities. The LA/OC HMIS Collaborative consists of four separate Continuums of Care (CoC). The continuums are: Los Angeles City and County; Santa Ana/Anaheim/Orange County; Glendale; and Pasadena.

The LA/OC HMIS Collaborative's goal is to provide a comprehensive case management system to advance the provision of quality services for homeless persons, improve data collection, and promote more responsive policies to end homelessness in the Greater Los Angeles and Orange Counties.

II. Agreement and Understanding

This Agreement authorizes you, an HMIS User (User), to enter Protected Personal Information (PPI) into the LA/OC 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/OC 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 his or her PPI entered into the LA/OC HMIS must sign the *Consent to Share Protected Personal Information* form.

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

III. Client Rights

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

- A copy of his or her consent form;
- A copy of his or her HMIS records; and
- A current list of participating organizations that have access to HMIS data.

IV. User Responsibilities and Conduct

I understand and agree that:

- I have an ethical and a legal obligation to ensure that the data I collect and enter into HMIS is accurate and does not misrepresent the client's information.
- I will not reveal or release PPI to unauthorized organizations, individuals or entities.
- I will use the data within the HMIS only for the purposes of homeless service delivery.
- I am not permitted to access the HMIS from any computer that has not been designated or approved by my organization.
- I will never use the HMIS to perform an illegal or malicious act.
- I will not attempt to increase the level of access to which I am authorized, or attempt to deprive other HMIS Users of access to the HMIS.
- My HMIS User ID and password shall be kept secure and will not be shared.
- I will refrain from leaving my computer unattended while logged into the system.
- I will protect and store client information printed from HMIS in a secure location.
- I will dispose of PPI printed from HMIS, when it is no longer needed, in a manner that maintains client confidentiality.
- If I suspect or encounter a security breach, I will immediately notify my organization's HMIS administrator.
- If my relationship with my organization changes or terminates, any client information that I entered into or obtained from the HMIS must remain confidential.
- Discriminatory comments based on race, color, religion, national origin, ancestry, handicap, age, sex and sexual orientation are not permitted in the HMIS. Profanity and offensive language are also not permitted in the HMIS.
- PPI that is transmitted electronically must be password protected to maintain confidentiality.
- I will comply with my organization's policies and procedures and the LA/OC HMIS Collaborative Policies and Procedures in my use of HMIS. The LA/OC HMIS Collaborative Policies and Procedures can be access from your CoC HMIS website.
- Any violation of this User Agreement is grounds for immediate suspension or revocation of my access to the HMIS.

My signature below confirms my agreement to comply with all the provisions of this Greater Los Angeles and Orange County 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 & ORANGE COUNTY
HOMELESS MANAGEMENT INFORMATION SYSTEM (LA/OC HMIS)

CONSENT TO SHARE PROTECTED PERSONAL INFORMATION

The LA/OC HMIS is a local electronic database that securely record information (data) about clients accessing housing and homeless services within the Greater Los Angeles and Orange Counties. 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 organization has signed an agreement to maintain the security and confidentiality of the information. In some instances, when the participating organization 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. Upon receipt of your revocation, we will remove your PPI from the shared HMIS database and prevent further PPI from being added. The PPI that you previously authorized to be shared cannot be entirely removed from the HMIS database and will remain accessible to the limited number of organization(s) that provided you with direct services.
- The Privacy Notice for the LA/OC 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.

SIGNATURE AND ACKNOWLEDGEMENT

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

☐ **I consent to sharing my photograph. (Check here)**

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

Signature _____Date _____

☐ **Head of Household (Check here)**

Minor Children (if any):

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

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

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

_____ _____

Print Name of Organization Staff **Print Name of Organization**

_____ _____

Signature of Organization Staff **Date**

Appendix D: Privacy Notice

GREATER LOS ANGELES & ORANGE COUNTY
HOMELESS MANAGEMENT INFORMATION SYSTEM (LA/OC HMIS)

PRIVACY NOTICE

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

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

Why We Collect and Share Information

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

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

The Type of Information We Collect and Share in the HMIS

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

- Name and contact information
- Social security number
- Birthdate
- Demographic information such as gender and race/ethnicity
- History of homelessness and housing (including current housing status and where and when services have been accessed)
- Self-reported medical history including any mental health and substance abuse issues
- Case notes and services
- Case manager's contact information
- Income sources and amounts; and non-cash benefits
- Veteran status
- Disability status
- Household composition
- Emergency contact information
- Domestic violence history
- Photo (optional)

How Your Personal Information Is Protected in the HMIS

Your information is protected by passwords and encryption technology. Each HMIS user and participating 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 organization.
- 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/OC 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/OC 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. Upon receipt of your revocation, we will remove your PPI from the shared HMIS database and prevent further PPI from being added. The PPI that you previously authorized to be shared cannot be entirely removed from the HMIS database and will remain accessible to the limited number of organization(s) that provided you with direct services.

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/OC 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.

Your Privacy Rights Regarding Your Information in the HMIS

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

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

Amendments to this Privacy Notice

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

Appendix E: Note Regarding Collection of Personal Information

GREATER LOS ANGELES & ORANGE COUNTY
HOMELESS MANAGEMENT INFORMATION SYSTEM (LA/OC HMIS)

NOTE REGARDING COLLECTION OF PERSONAL INFORMATION

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

A Privacy Notice is available upon request.

Appendix F: Revocation of Consent

GREATER LOS ANGELES & ORANGE COUNTY
HOMELESS MANAGEMENT INFORMATION SYSTEM (LA/OC HMIS)

REVOCATION OF CONSENT

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

I understand that this revocation authorizes the removal of my PPI from the shared HMIS database and will prevent further PPI from being added. I understand that the PPI that I previously authorized to be shared cannot be entirely removed from the HMIS database and will remain accessible to the limited number of organization(s) that provided me with direct services.

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_____

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**

Last updated on: 10/29/2015

Appendix G: Interagency Data Sharing Consent Form

GREATER LOS ANGELES & ORANGE COUNTY
HOMELESS MANAGEMENT INFORMATION SYSTEM (LA/OC HMIS)

INTERAGENCY DATA SHARING CONSENT FORM

Client Name:_____

SSN/Client ID:_____

Date of Birth:_____

Name of Originating Organization:_____

Name of Organization with which to extend Client Data Sharing:

_____

Client Information to Share **(Client: please INITIAL all forms you want to share)**:

____Program Entry Required Questions
____Services Provided
____Case Notes
____Assessment (Client Profile)
____Savings Record
____Program Exit Information
____Group Meetings
____Any information as necessary

_____

Client Signature Date

Appendix H: Grievance Form

GREATER LOS ANGELES & ORANGE COUNTY
HOMELESS MANAGEMENT INFORMATION SYSTEM (LA/OC HMIS)

GRIEVANCE FORM

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

Grievances must be submitted in writing to:
[Enter Address]

Date of offense: _____

_____	_____
Name of Individual who violated your privacy rights.	Name of Organization who violated your privacy rights.

Brief description of grievance (what happened):

Best way to contact you: _____

Your name: _____

Your phone: _____

Your mailing address: _____

_____

CoC response date: _____

Recommendation to Organization:

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

Last updated on: 10/29/2015

Appendix I: Client's Rights Brochure

For Further Homeless Provider Information and Assistance

2-1-1 Orange County
1505 E 17th Street Suite 108
Santa Ana, CA 92705
(714) 288-4007
www.211oc.org

OC Community Services
1770 N. Broadway
Santa Ana, CA 92706
(714) 480-2900

Last updated 10/07/2015

Greater Los Angeles and Orange Counties Homeless Management Information System (HMIS)

Mission: Leveraging technology in a respectful and appropriate manner, HMIS will assist homeless providers, persons experiencing a housing crisis, and policy advocates to end homelessness in the Greater Los Angeles and Orange counties.

Vision: The LA/OC Collaborative is dedicated to providing the best possible, highest quality Homeless Management Information System (HMIS) to enhance the Continuum of Care for persons experiencing homelessness. Specifically, HMIS will:

- Enable providers to **track services, report outcomes, and manage** client data using accessible and user-friendly technology
- Enhance the ability of policy makers and advocates **to gauge the extent of homelessness and plan services** appropriately throughout the Greater Los Angeles and Orange counties
- Ensure persons experiencing a housing crisis receive **streamlined referral, coordinated services, and speedy access** to essential services and housing

Homeless Management Information System (HMIS)

Client Rights & Explanation of Data Uses

For more information, contact the HMIS Administrative Office
(714) 288-4007
www.211oc.org

HMIS

What Is HMIS?

The Homeless Management Information System (HMIS) is a web-based information system. Organizations that serve homeless and at-risk individuals in the Greater Los Angeles and Orange counties need to compile information about the persons they serve.

Why Gather and Maintain Data?

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

Consent

Written Client Consent

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

Client Rights

Common Client Questions:

Who can access my information?

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

Who will receive my information?

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

Don't I have a right to privacy?

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

What if I don't want to provide information?

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

What if I believe my rights have been violated?

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

Grievance

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

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

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

Acknowledgement

I acknowledge that I have received a written copy of the LA/OC HMIS Collaborative Policies and Procedures Manual. I understand the terms of the LA/OC HMIS Policies and Procedures and I agree to abide by them. I understand that any violation of the policies or procedures could lead to my HMIS account being locked or even criminal prosecution.

Organization Name: _____

Printed Name: _____

Signature: _____

Date: _____