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

TABLE OF CONTENTS

TABLE OF CONTENTS **2**

HMIS LEAD AGENCIES CONTACT INFORMATION **4**

City of Glendale 4
City of Pasadena 5
Los Angeles Homeless Services Authority (LAHSA) 6
Orange County 7

PROJECT SUMMARY **8**

Background 8
LA/OC HMIS Collaborative 8
Mission Statement 9
Vision 9
LA/OC HMIS Software 9

1. ROLES AND RESPONSIBILITIES **10**

1.1 LA/OC HMIS Collaborative Responsibilities 10
1.2 HMIS System Administrator Responsibilities 10
1.3 Agency Administrator Responsibilities 10
1.4 HMIS Security Officer Responsibilities 11
1.5 HMIS Lead Agency Communication with Participating Agency 11
1.6 Participating Agency Communication with HMIS Lead Agency 12

2. IMPLENTATION POLICIES AND PROCEDURES **13**

2.1 HMIS Agency 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 16
2.6 HMIS Technical Support Protocol 16
2.7 System Availability 17
2.8 Participation Fees 17

3. SECURITY POLICIES AND PROCEDURES **18**

3.1 User Authentication 18
3.2 Passwords 18
3.3 Extracted Data 19
3.4 Encryption Management 19
3.5 Hardware Security Measures 20
3.6 Backup and Recovery Procedures 20
3.7 Security Review 21
3.8 Security Violations and Sanctions 21

4. OPERATIONAL POLICIES AND PROCEDURES **22**

4.1 User Access Levels 22
4.2 Training 23
4.3 User Guide 24
4.4 Client Informed Consent and Confidentiality 24
4.5 Client Revocation of Consent to Release Information 25
4.6 Data Sharing 26
4.7 Client Record Access 26
4.8 Client Grievance 27

5. DATA POLICIES AND PROCEDURES 28

6. TERMINOLOGY 31

7. APPENDICES 35

Appendix A: HMIS Agency Agreement 36
Appendix B: HMIS User Agreement 40
Appendix C: Client Consent and Information Release 42
Appendix D: Privacy Notice 44
Appendix E: Mandatory Collection Notice 45
Appendix F: Client Revocation of Consent to Release Information 46
Appendix G: Interagency 47
Appendix H: Grievance Form 48

ACKNOWLEDGEMENT 49

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) 548-2000
Fax: (818) 548-3720

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 System Administrator	cbrooks@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 System 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
http://lahsahmis.esserver.com/

Orange County

Orange County has its own Continuum of Care.

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

Tel: (714) 288-4007
Fax: (714) 258-7852

HMIS Contact Information		
Team	**Contact Email**	**Reason**
HMIS Assistance	helpdesk@ocpartnership.net	

OC HMIS Website
http://ochmis.org/

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

OC HMIS Version 5
http://ochmis.esserver.com/

PROJECT SUMMARY

Background

In 2001, Congress directed the US Department of Housing and Urban Development (HUD) regarding the need for data and analysis on the extent of homelessness. HUD requires each Continuum of Care (CoC) to have a Homeless Management Information System (HMIS) designed to facilitate data collection.

Below are HUD funded programs required to participate in the HMIS:

- Emergency Solutions Grant (ESG)
- Housing Opportunities for People with AIDS (HOPWA)
- Continuum of Care Program (comprises the Supportive Housing Program, Shelter Plus Care Program, and the Single Room Occupancy Program)

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.

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 Continuums 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.

- OC Partnership and its partners Orange County Housing & Community Services Department and 211 Orange County 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 end 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
- Client demographic data collection
- Comprehensive client case management
- Customized assessment capability
- Customized reporting capability
- Employment, education, and housing history tracking
- Group activities management
- Group case notes management
- Information and referral capabilities
- Outcome management
- Outreach
- Real-time data collection and reporting
- Savings tracking

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:

- The HMIS System Administrator is the primary position at the LA/OC Collaborative for HMIS management.

1.2 HMIS System Administrator Responsibilities

Policy:

HMIS System Administrators will provide training and technical support to Participating Agencies.

Responsibilities:

The HMIS System Administrator is responsible for:

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

Procedure:

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

1.3 Agency Administrator Responsibilities

Policy:

Each Participating Agency must designate an Agency Administrator and a backup Agency 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 Agency Administrator is responsible for:

- Serving as the primary contact between end users and HMIS System Administrator;
- Providing technical support by troubleshooting data and escalating unresolved issues to the HMIS System Administrator;
- Notifying all members of their agency of any system-wide changes and other relevant information;
- Conduct training to end users if applicable to the local agency's region;
- Notifying the HMIS System Administrator of personnel changes;
- Monitoring compliance with standards of confidentiality and data collection, entry, and retrieval;
- Ensuring that all authorized end 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 Agency must provide their local HMIS Lead Agency the name and contact information of the Agency Administrator and backup Agency Administrator.
- Any changes to that information must be reported to the HMIS System Administrator.

1.4 HMIS Security Officer Responsibilities

Policy:

Each HMIS Lead Agency and Participating Agency must designate a HMIS Security Officer to be responsible for ensuring compliance with the security standards outlined in the Policies and Procedures described in this document.

Procedure:

- Each HMIS Lead Agency and Participating Agency will assign one employee as the HMIS Security Officer.
- The designated employee will be subject to a criminal background check.

1.5 HMIS Lead Agency Communication with Participating Agency

Policy:

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

Procedure:

- HMIS System Administrators will send email communication to the Agency Administrator.
- Agency Administrators are responsible for distributing information and ensuring that all members of their agency 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.

1.6 Participating Agency Communication with HMIS Lead Agency

Policy:

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

Procedure:

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

2. IMPLENTATION POLICIES AND PROCEDURES

2.1 HMIS Agency Agreement Requirement

Policy:

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

Procedure:

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

2.2 HMIS User Agreement Requirement

Policy:

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

Procedure:

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

2.3 Data Collection Requirements

Policy:

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

Procedure:

- Participating Agencies must enter data into the system within 3 days of collecting the information.
- In Central Intake, end users must collect all the universal data elements set forth in the HMIS Data Standards Revised Notice, March 2010.

The universal data elements include:

- Name
- Social Security Number
- Date of Birth
- Race
- Ethnicity
- Gender
- Veteran Status
- Disabling Condition
- Residence Prior to Program Entry
- Zip Code of Last Permanent Address
- Housing Status
- Program Entry Date
- Program Exit Date

- End users must also collect all the program-specific data elements at program entry and exit set forth in the HMIS Data Standards Revised Notice, March 2010. The program-specific data elements include:

  - Income and Sources
  - Non-Cash Benefits
  - Physical Disability
  - Chronic Health Condition
  - HIV/AIDS
  - Mental Health
  - Substance Abuse
  - Domestic Violence
  - Services Provided
  - Destination (Program Exit)
  - Reason for Leaving (Program Exit)

- These standards are already required fields in the LA/OC HMIS.

2.4 Technical and Security Standards

Policy:
Participating Agencies 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 Upload Speed
75% Quality of Service	90% Quality of Service

Compatible Operating Systems and Browsers					
Operating Systems	**IE 9**	**IE 8**	**IE 7**	**Firefox 4+**	**Chrome 11+**
Windows Vista	X	X	X	X	X
Windows 7	X	X		X	X
Windows XP SP2, SP3		X	X	X	X
Macintosh OS 10.4.11+ (Intel based)				X	X

Minimal Microsoft Requirements	
Windows	**Mac**
.NET 2.0 SP2	MS Silverlight 4.0
.NET 3.0 SP2	Silverlight must be installed on the computer before using HMIS, please visit Silverlight Installation website: http://www.microsoft.com/getsilverlight
.NET 3.5 SP1	
MS Silverlight 4.0	

- Connection to the internet is the sole responsibility of the Participating Agency and is a requirement to participate in the LA/OC HMIS.
- All Operating systems should have the latest SP applied. Network design should allow for uninterrupted communication between App, 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 Agencies 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.
    - Workstation accessing the system must have a static IP address.
    - All workstations and computer hardware (including agency network equipment must be stored in a secure location (locked office area).

2.6 HMIS Technical Support Protocol

Policy:

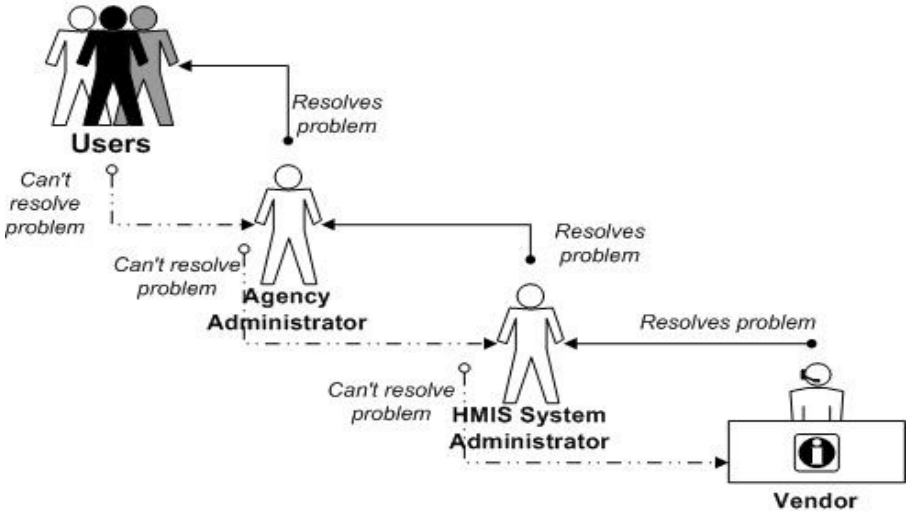
Each HMIS Lead Agency will provide technical support to all Participating Agencies as needed.

Procedure:

1. End users should first seek technical support from the Agency Administrator.
2. If more expertise is required to further troubleshoot the issue, Agency Administrator will contact the HMIS System 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 Agency Administrator will provide issue details if possible (or help recreate the problem by providing all information, screenshots, reports, etc.) in order for the HMIS System Administrator to recreate the problem.
5. The HMIS System 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 System 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



2.7 System Availability

Policy:

The LA/OC HMIS will be available to end users at a minimum of 97.5% of the year. The vendor and the HMIS Lead Agency will inform end 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 System Administrators will analyze and determine the problem.
- The HMIS System Administrator will work with the software vendor to repair the problem.
- The HMIS System Administrators will send email communication to the Agency Administrator within 2 hours of problem awareness and informed them of estimated 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 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 System 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 Agency 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 end user must complete the required training and demonstrate proficiency in use of system.
- Proposed end 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 System 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 System 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.
- Agency Administrator is required to notify the HMIS System Administrator when end user leaves employment with the agency or no longer needs access.
- HMIS System Administrator will terminate access upon notification of the Agency Administrator.

3.2 Passwords

Policy:

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

Procedure:

- The HMIS System Administrator will provide new end users a unique username and temporary password after required training is completed.
- End 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 end user will be prompted to enter a new password. End users may not use the same password consecutively, but may use the same password more than once.
- After 10 minutes of inactivity, end users 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.
- Access permission will be revoked after the end user unsuccessfully attempts to log on three times. The end user will be unable to gain access until password is reset by the HMIS System Administrator.
- The Agency Administrators will need to contact the HMIS System Administrator to regain access or to reset the password for end user.

3.3 Extracted Data

Policy:

End 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. End 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 System 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 System Administrator, on behalf of the vendor, will obtain the written permission of the Executive Management of each Participating Agency 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 Agencies 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 Agency 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 System 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 System 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 Agencies.

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 end user found to be in violation of security protocols of the agency procedures or Policies and Procedures will be sanctioned accordingly. All end users must report potential violations of any security protocols described in the Policies and Procedures.

Procedure:

- End users are obligated to report suspected instances of noncompliance and/or security violations to the Agency Administrator or HMIS System Administrator as soon as possible.
- The Agency Administrator or HMIS System Administrator will investigate potential violations.
- Any end 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:

Each end 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 System Administrator, in consultation with the Participating Agency, will assign the level and type of access the user will have in the system.
- Agency Administrator is required to communicate to HMIS System Administrator when end user's need for access changes.
- HMIS System Administrator will terminate access upon notification and receipt of Termination of Employee Form from the Agency Administrator.
- HMIS System 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 that may be offered in consultation and with approval from the HMIS System Administrator (See HMIS Lead Agencies Contact Information).

User Role	Level of Access	Description
HMIS System 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 agencies, meet reporting requests, and other system administration responsibilities.
Agency Administrator	Access to Central Intake, Agency Services, and other system libraries.	This role will grant access to data collected by their own agency.
Case Manager	Access to Central Intake and Agency Services libraries.	This role will grant access to data collected by their own agency.
Client Data Entry	Access only to Central Intake Library.	This role will grant access only to Central Intake for intake purposes.
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 end user must complete the required training and any additional training relevant to their position prior to gaining access to the LA/OC HMIS. HMIS System Administrators will provide training to all end users.

Procedure:

- HMIS System Administrator will provide Basic User Training to proposed end users. Agency Administrator may be trained to provide Basic User Training to support agency personnel if applicable for the local agency's region. Consult local HMIS Lead Agency (See HMIS Lead Agencies Contact Information).
- End users must successfully complete the Basic User Training and pass the exam to demonstrate proficiency in the system and understanding of the Policies and Procedures.
- HMIS System Administrator will provide new end user with a copy of the Policies and Procedures and HMIS Users Guide.
- 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 Agencies, 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 end users.
Ethics and Confidentiality Training	This course focuses on ethics and confidentiality.	All new end users.
Security Training	*This will be a new course based on the upcoming Federal Regulations.	All new and existing users.
Agency Administrator Training		Agency Administrators
Outcome Management Training		Outcome Specialists
Reporting Training	This course focuses on management reports.	

4.3 User Guide

Policy:

Each end user will receive a copy of the LA/OC HMIS User Training Manual.

Procedure:

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

4.4 Client Informed Consent and Confidentiality

Policy:

Participating Agencies must obtained informed, signed consent prior to entering any client personal identifiable information 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 Agency and end user must abide by the terms in the HMIS Agency Agreement and HMIS User Agreement.

Procedure:

- Client must sign Informed Consent Information Release Authorization Form (Appendix C) or consent of the individual for data collection may be inferred from the circumstances of the collection. Participating Agencies may use the Mandatory Collection Notice (Appendix E) to meet this standard.
- Clients that provide permission to enter personal information allow for Participating Agencies within the region to share client and household demographic data. Sharing of program level client data between Participating Agencies will require a signed Interagency Sharing Agreement.
- Participating Agencies must store signed Informed Consent Information Release Authorization Form in client record for auditing purposes.
- Participating Agencies must post a Privacy Notice (Appendix D) and a Mandatory Collection Notice (Appendix E) that explains the uses and disclosures of information.
- If client refuses consent, the end user should not include any personal identifiers (First Name, Last Name, Social Security Number, and Date of Birth) in the client record.
- For clients with consent refused, end user should include a client identifier to recognize the record in the system.
- Participating Agencies shall uphold Federal and State Confidentiality regulations and laws that protect client records.

Applicability:

DMH County legal guidance has ruled that DMH is a HIPAA covered entity and must use DMH-prescribed forms for client consent for data collection and client authorization to have client data entered into HMIS. This is in accordance with the 2004 HMIS Data and Technical Standards Final Notice (Federal Register, Volume 69. No. 140, Friday July 30, 2004, pp. 45888-45934).

The HMIS standards and the HIPAA standards are mutually exclusive. 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.

The forms identified below will not be used by DMH (only):

- Client Consent and Information Release Form
- Notice of Privacy Practices
- Mandatory Collection Notice
- Grievance Forms

DMH and end users will still be subject to the HMIS Agency Agreement and HMIS User Agreement.

4.5 Client Revocation of Consent to Release Information

Policy:

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

Procedure:

- Upon request, the Participating Agency 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.
- End user should include a client identifier to recognize the record in the system.

4.6 Data Sharing

Policy:

Client data (with consent) contained in Central Intake Library will be shared with other Participating Agencies. Sharing of program level client data between Participating Agencies will require a signed Interagency Sharing Agreement. Client may choose to limit the period of time for which their data will be shared.

Procedure:

- Data sharing refers to the sharing of information between Participating Agencies for the coordination of case management and client service delivery.
- Client data in the Central Intake includes:
    - Universal Data Elements
    - Household Demographics
    - Employment and Education Information
- Sharing of program level client data between Participating Agencies will require a signed Interagency Sharing Agreement (Appendix G).
- Participating Agencies must store signed Interagency Sharing Agreement in client record for auditing purposes.
- End users found to be sharing program level client data without written 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 Agency, 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 agency the client requests it from, as long as the client has previously given the other agency consent to share and that consent is still in force. The Participating Agency may not share any client information entered by other agencies beyond the Central Intake Library.
- The Agency 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 personal identifiable information be removed from the system. In response, the Agency Administrator will remove such data from record within 3 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 agency guidelines.

4.8 Client Grievance

Policy:

Clients will file LA/OC HMIS-related grievances with the Participating Agency. The Participating Agency 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 Agency with which they have a grievance.
- Upon client request, the Participating Agency will provide a copy of their grievance procedure and the LA/OC HMIS Policies and Procedures.
- The Participating Agency 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 Agency will include the date and a brief description of the resolution. For any written complaint, the Participating Agency must send a copy to the local HMIS Lead Agency.
- If the Participating Agency 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 Agency 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:

End 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 Agencies must sign the HMIS Agency Agreement to ensure that all participating programs are aware and have agreed to the data quality standards.
- Upon agreement, Participating Agencies 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 three (3) days of program entry.
- The HMIS System Administrator will conduct random checks for data quality. Any patterns of error or missing data will be reported to the Agency Administrator.
- End users will be required to correct the identified data error and will be monitor for compliance by the Agency Administrator and the HMIS System Administrator.
- End users may be required to attend additional training as needed.

5.2 Data Use and Disclosure

Policy:

All end 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 agency. Disclosures involve sharing parts of client information with persons or organizations outside an agency.

Procedure:

- Participating Agencies may use data contained in the system to support the delivery of services to homeless clients in the Los Angeles and Orange Counties. Agencies may use or disclose client information internally for administrative functions, technical support, and management purposes. Participating Agencies 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 Agency owns all data that is stored in the system. The agency may not release personal identifiable client data without written permission from the client. Agencies may release program and/or aggregate level data for all clients to whom the agency provided services. No personal identifiable client data will be provided to any group or individual that is neither the Participating Agency 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 agency 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 from legacy systems is allowed upon approval from the HMIS System Administrators. Migrated data must be non-duplicated and an exact match to the existing field type of the LA/OC HMIS. The Participating Agency will be responsible for the accuracy, completeness, and quality of the migrated data.

Definition:

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

Procedure:

- The existing system of the Participating Agency must be an ODBC-compliant database platform in order for migration to be possible. The HMIS System Administrator can help the agency 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 System Administrator will decide the appropriate data migration candidates. If approved, a Transfer of Data Agreement must be completed and the Agency will provide current data in an ODBC usable form to the HMIS System Administrator.
- If the data cannot be migrated, manual conversion (data entry by the agency'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 agency.

6. TERMINOLOGY

Adsystech: Software developer of the RESULTBase ODM software used by TRI for the LA/OC HMIS.

Agency Administrator: The person responsible for System administration at the agency 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 System Administrator. This person is the agency user's first line of contact for LA/OC HMIS issues.

Agency Executive Management: The high-level management staff that is responsible for organization level decision making, for example, the agency President or Executive Director.

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.

Application Service Provider (ASP): A 3rd party entity that manages and distributes software-based services to customers across a wide area network.

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.

Cable: A type of modem that allows people to access the Internet via their cable television service.

Central Intake level data: Client information collected at intake, including the following system screens: Client Intake, Household/Demographics, Referral, Eligibility, Education/Employment and Documents.

Change Management Committee: A subgroup of the LA/OC Collaborative, including one technology representative, one program representative, and one policy representative.

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

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

CoC Governing Body: the entity responsible for policy decisions for a Continuum of Care system.

Continuum of Care (CoC) Level: There are four Continuum of Care (CoC) systems in the LA/OC HMIS Collaborative.

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.

Dedicated IP: a reserve IP (see IP)

Dynamic Host Configuration Protocol (DHCP): A protocol that provides a means to dynamically allocate IP addresses to computers on a local area network (LAN). The system administrator assigns a range of IP addresses to DHCP and each client computer on the LAN has its TCP/IP software configured to request an IP address from the DHCP server.

Digital Certificate: An attachment to a message or data that verifies the identity of a sender.

Digital Subscriber Line (DSL): A digital telecommunications protocol designed to allow high-speed data communication over the existing copper telephone lines.

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 System 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 Agencies and the vendor. There is at least one HMIS System Administrator in each CoC.

HMIS System Administrator Committee: The HMIS System Administrator Committee is made up of representatives from agencies throughout the collaborative, including agency administrators and other technical staff. The committee provides recommendations and feedback to the LA/OC HMIS Steering Committee for technical procedures and system integration protocols for the LA/OC HMIS.

HMIS User: A person 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 agency users who perform functions at the agency level.

Host: A computer system or organization that plays a central role providing data storage and/or application services for the LA/OC HMIS.

Internet: A set of interconnected networks that form the basis for the World Wide Web.

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.

Los Angeles/Orange County (LA/OC) HMIS Collaborative: The entity responsible for recommending the selection, implementation and adherence to standards of the local HMIS. The LA/OC HMIS Collaborative is comprised of representatives from each of the five regions within the coordinating body. These regions include the Los Angeles Homeless Services Authority, the City of Pasadena, the City of Glendale, and Orange County.

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.

Network Address Translation (NAT) is the translation of an Internet Protocol address (IP address) used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside. Typically, a company maps their local network addresses to one or more global outside IP addresses and un-maps the global IP addresses on incoming packets back into local IP addresses. This helps ensure security since each outgoing or incoming request must go through a translation process that also offers the opportunity to qualify or authenticate the request or match it to a previous request. NAT also conserves on the number of global IP addresses that a company needs and it lets the company use a single IP address in its communication with the world.

On-site: The location that uses the LA/OC HMIS and provides services to at-risk and homeless clients.

Outcome Manager: The person at each Participating Agency designated to develop and assess the use of outcome measures for the agency's data on the LA/OC HMIS.

Outcome Specialist: The person(s) in each CoC who provide the agency's Outcome Managers with training and technical assistance (TA) for outcome management. The Outcome Specialist will serve as the liaison between Participating Agencies and the local CoC Governing Body in the development of performance targets and milestones for each program that is entered in the LA/OC HMIS. There is at least one Outcome Specialist in each CoC.

Participating Agency: An agency, organization or group that has signed an HMIS Agency Agreement with their respective CoC Governing Body and is allowed access to the LA/OC HMIS. These agencies connect independently to the LA/OC HMIS via the Internet.

Program and Policy Committee: The Program and Policy Committee is comprised of representatives from agencies throughout the collaborative, including program managers, case managers and other agency staff. The committee provides recommendations and feedback to the LA/OC HMIS Steering Committee for policies and procedures, data elements and reporting protocols for the LA/OC HMIS.

Program Level Data: Client information collected during the course of the client's program enrollment, including the following system screens: Program Entry, Services Provided, Client Profile, Case Notes, Track Savings, Bed Assignments, Bed

Maintenance, Daily Services, Sessions, and Program Exit.

Real-Time: Data that is processed and available to other users as it is entered into the system.

ResultBase ODM ™: The software package provided by the vendor that has been implemented as the LA/OC HMIS solution.

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.

Static IP Address: see Dedicated IP

T1 Line: Communication line that can carry voice or data at transmission speeds that are 25 times the speed of a modem.

Transmission Control Protocol/Internet Protocol (TCP/IP) –The protocol that enables two or more computers to establish a connection via the internet.

TRI: The Rensselaerville Institute of Rensselaerville, NY is the vendor providing the LA/OC HMIS solution to be used by the LA/OC region.

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

Virtual Private Network (VPN): A group of computer systems that communicate securely over a public network.

Wide Area Network (WAN): A network that is not geographically limited, can link computers in different locales, and extend requests for web pages.

Wired Equivalent Privacy (WEP): A security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) Standard, 802.11b that is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN. A wired local area network (LAN) is generally protected by physical security mechanisms (controlled access to a building, for example) that are effective for a controlled physical environment, but may be ineffective for WLANs because radio waves are not necessarily bound by the walls containing the network. WEP seeks to establish similar protection to that offered by the wired network's physical security measures by encrypting data transmitted over the WLAN. Data encryption protects the vulnerable wireless link between clients and access points; once this measure has been taken, other typical LAN security mechanisms such as password protection, end-to-end encryption, virtual private networks (VPNs), and authentication can be put in place to ensure privacy.

7. APPENDICES

Appendix	Document Title
Appendix A	HMIS Agency Agreement
Appendix B	HMIS User Agreement
Appendix C	Client Consent and Information Release
Appendix D	Privacy Notice
Appendix E	Mandatory Collection Notice
Appendix F	Client Revocation of Consent to Release Information
Appendix G	Interagency Data Sharing Consent Form
Appendix H	Grievance Form
Appendix I	Client Rights Brochure

Appendix A: HMIS Agency Agreement

Los Angeles/Orange County
Homeless Management Information System (HMIS) Collaborative

HMIS Agency Agreement

I. Purpose

The Los Angeles/Orange County (LA/OC) Homeless Management Information System (HMIS) is a web-enabled database used by homeless service providers within the Los Angeles and Orange County region, to capture information about the persons they serve. The LA/OC HMIS Collaborative consist of four separate Continuum of Cares. The continuums are: Los Angeles Homeless Service Authority (LAHSA), Orange County Continuum of Care, the City of Glendale and the City of Pasadena.

The LA/OC HMIS Collaborative's goal is to go beyond the HUD mandate of producing unduplicated counts of homeless persons. Our mission 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 Los Angeles and Orange Counties.*

II. Audience and Agreement

This Participating Agency Agreement permits (Agency Name) and its participants to use the LA/OC HMIS and security services on their computers systems through an Internet connection. The LA/OC HMIS Collaborative and their assigned HMIS System Administrators are the primary coordinating Continuum of Cares (CoC) for the LA/OC HMIS. The Participating Agency is the "Agency" named in this agreement as participants of the LA/OC HMIS. The HMIS "User" are the guardians entrusted with personal data to be entered and used in the LA/OC HMIS and the "Client" is the consumer of services.

All agencies which have been granted access to the LA/OC HMIS have agreed to abide by all laws, and the LA/OC HMIS Collaborative Policies and Procedures pertaining to client confidentiality, user conduct, security, and the ongoing functionality and stability of services and equipment used to support the LA/OC HMIS.

The signature of the Executive Director of the Participating Agency indicates agreement with the terms set forth for an LA/OC HMIS account for the Agency.

III. Confidentiality and Informed Consent

The Agency agrees to abide by and uphold all privacy protection standards established by the LA/OC HMIS Collaborative as well as their respective agency's privacy procedures. The Agency will also uphold relevant Federal and California State confidentiality regulations and laws that protect client records, and the Agency will only release confidential client records with written consent by the client, or the client's guardian, unless otherwise provided for in the regulations or laws. Access to the LA/OC HMIS is granted to the (agency name) based on the following premises:

Oral Explanation: All clients will be provided an oral explanation stating their information will be entered into a computerized record keeping system. The Agency will provide an oral explanation of the LA/OC HMIS and the terms of consent. The agency is responsible for ensuring that this procedure takes place prior to every client interview.

Written Explanation: Each client whose information is being shared with another participating agency must agree via the written Client consent/Information Release form. A client must be informed as to what information is being shared and with whom it is being shared.

Information Release: The Agency agrees not to release client identifiable information to any other organization without proper client consent except as provided by federal and California State law. See attached Client Consent/Information Release Form and Regulations below.

Regulations: The Agency will uphold all relevant Federal and California State confidentiality regulations to protect client records and privacy. In addition, the Agency will only release client

records with written consent by the client, unless otherwise provided for in the regulations. Specifically, but not limited to, the following:

A. The Agency will abide specifically by the federal confidentiality rules as contained in the Code of Federal Regulations (CFR) 42 Part 2 Confidentiality of Alcohol and Drug Abuse Patient Records, regarding disclosure of alcohol and/or drug abuse records. In general terms, the Federal regulation prohibits the disclosure of alcohol and/or drug abuse records unless disclosure is expressly permitted by written consent of the person to whom it pertains or as otherwise permitted by CFR 42 Part 2. A general authorization for the release of medical or other information is not sufficient for this purpose. The Agency understands that the Federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patients.
B. The Agency will abide specifically with the Health Insurance Portability and Accountability Act of 1996 and corresponding regulations passed by the U.S. Department of Health and Human Services. In general, the regulations provide consumers with new rights to control the release of medical information, including advance consent for most disclosures of health information, the right to see a copy of health records, the right to request a correction to health records, the right to obtain documentation of disclosures of information may be used or disclosed. The current regulation provides protection for paper, oral, and electronic information.
C. The Agency will abide specifically with the California Government Code 11015.5 regarding Personal Information Collected on the Internet. In general, the Government Code ensures that any electronically collected personal information about clients cannot be shared with any third party without the client's written consent.

Postings: Privacy and Mandatory Collection notices must be posted at the agency.

A. The Agency must post Privacy and Mandatory Collection notices at each intake desk or comparable location.
B. Privacy and Mandatory Collection notices must be made available in writing at the client's request.
C. If the Agency maintains an agency website, a link to the privacy notice must be on the homepage of the agency's website.

IV. Data Use

Data contained in the LA/OC HMIS will only be used to support the delivery of homeless services in the Los Angeles and Orange County region. Each User will affirm the principles of ethical data use and client confidentiality as noted below and contained in the LA/OC HMIS User Agreement.

1. The Agency will not solicit or input information from clients unless it is essential to provide services, or conduct evaluation or research.
2. The Agency understands that all client data will be maintained on a central server, which will contain all client information in an encrypted state. All client identifiable data is inaccessible to unauthorized users.
3. The Agency shall not be denied access to client data entered by the Agency. Agencies are bound by all restrictions placed upon the data by the client of any Participating Agency. The Agency shall diligently record in the LA/OC HMIS all restrictions requested.
4. The Agency shall not knowingly enter false or misleading data under any circumstances.
5. The Agency shall maintain appropriate documentation of client consent to participate in the LA/OC HMIS.
6. If a client withdraws consent for release of information, the Agency remains responsible to ensure that the client's information is unavailable to all other Agencies.
7. The Agency shall keep signed copies of the Client Consent/Information Release form for LA/OC HMIS for a period of seven years.
8. The Agency shall keep Interagency data sharing agreements and Client Consent/Information Release forms for all individual client data that is shared to non-custodial agencies where the internal policies of the Agency allows data sharing.

V. Responsibilities

The Agency is responsible for ensuring that its staff does not intentionally or unintentionally misuse the system. Such uses are but not limited to damage computing resources, obtain extra resources, take resources from another user, gain unauthorized access to resources, or otherwise make use of computing resources for which proper authorization has not been given.

1. The Agency will have an environment free of illegal or malicious acts and the Agency's users agree to never use the system to perform an illegal or malicious act. Any attempt to increase the level of access to which (s)he is authorized or any attempt to deprive other authorized users of resources or access to LA/OC HMIS shall be regarded as malicious and may be treated as an illegal act.
2. Any user who finds a possible security lapse on the system is obligated to report it to the HMIS System Administrator immediately.
3. The LA/OC HMIS Application, which has been granted, to each participating agency was purchased by the LA/OC HMIS Collaborative for each of its own continuums. The LA/OC HMIS application was paid for through the HUD grant. The maintenance, upgrades and license purchases are limited by the sanctions of the HUD grant. Any additional maintenance, upgrades and license purchases incurred after the grant fund limit, which is designated for HMIS services, becomes the sole responsibility of the Agency that has accepted possession and use of the software and services rendered for HMIS purposes and functionality.

VI. System Usage

Computer Equipment and Services are intended for LA/OC HMIS-related activities. Acceptable computer system use includes data intake, reports, research of client, client development and public service purposes. Prohibited Usage includes, but is not limited to, the following activities: fraudulent, threatening, harassing, or obscene messages and/or materials are to be avoided and not to be received, sent nor stored. Inappropriate mass mailing (spamming, flooding, bombing) are prohibited. Creation or intentional distribution of computer viruses, worms, or Trojan horses is prohibited. Unauthorized access to or denial of service attacks on any computer system shall not be attempted. Abusers are subject to sanctions as outlined in Section XI. - Violations.

***Equipment if applicable**:* All of the computer equipment including, but not limited to, printers, scanners, laptops and monitors, which were purchased by your continuum of care for LA/OC HMIS purposes to all the participating agencies, are all under HUD grant funding. The maintenance and upgrades of these devices are limited by sanctions of the HUD grant. Any additional maintenance or upgrade costs incurred after the grant fund limit which is designated for LA/OC HMIS equipment becomes the sole responsibility of the Agency that has accepted possession and use of the equipment rendered for LA/OC HMIS purposes and functionality.

***Services if applicable**:* Which have been given to each participating agency are included but not limited to Anti-Virus Software and licenses, Firewall software and licenses, Windows software updates and High-Speed Internet Connections, are purchased by the LA/OC Collaborative for HMIS purposes and are all under HUD grant funding. The maintenance, upgrades and license purchases are limited by the sanctions of the HUD grant. Any additional maintenance, upgrades and license purchases incurred after the grant fund limit, which is designated for LA/OC HMIS services, becomes the sole responsibility of the Agency that has accepted possession and use of the software and services rendered for LA/OC HMIS purposes and functionality.

VII. Rights

LA/OC HMIS data from agencies within each continuum resides in one central database. The Agency's data is separated by security for each continuum. Data sharing is currently limited to the data within the Agency's continuum. The LA/OC HMIS Collaborative reserves the right, at a later date, to expand data sharing to include collaborative wide data.

The LA/OC HMIS Collaborative also reserves all rights, including termination of agreements, of the LA/OC HMIS application and the service resources that it owns and operates. These procedures shall not

be construed as a waiver of any rights of the LA/OC HMIS Collaborative, nor shall they conflict with applicable acts of law.

VIII. Privileges

The LA/OC HMIS services and or equipment are a privilege and are assigned and managed by the HMIS System Administrator(s) or designee(s) of specific systems. The Agency is responsible for proper use of the system as outlined in Section VI.

IX. Confidentiality

Although technological and procedural securities have been reasonably exhausted by the LA/OC HMIS Collaborative to ensure client data confidentiality, this system is being used by a multitude of end users and is therefore subject to the diligence to which the Participating Agencies' staff protects client records.

The protections that the LA/OC HMIS Collaborative put in place to protect client confidentiality include compliance with HUD Data and Technical Standards Final Notice, institution of a mandated HMIS training program for all HMIS users, consistent application of Policies and Procedures, and signed Agency End-User Agreements.

X. Copyright

The LA/OC HMIS is protected by copyright and is not to be copied, except as permitted by law or by contract with owner of the copyright. The number of copies and distribution of copies are to be managed by the HMIS Systems Administrator(s) of each CoC. Interference with measures used by copyright holders to protect copyrighted works is prohibited.

Agency user's storing materials copyrighted by others on the systems or displaying the materials through web pages must comply with copyright laws and guidelines.
***Equipment if applicable*:** Computer software and data are protected by copyright and is not to be copied, except as permitted by law or by contract with the owner of the copyright. The number of copies and distribution of copies are to be managed by the HMIS Systems Administrator(s) of each CoC. Users of the computer systems agree to follow guidelines for use of copyrighted materials.

XI. Violations

An individual violating any of the guidelines outlined in this agreement will be reported immediately upon discovery. Such suspected violations will be confidentially reported to the HMIS System Administrator(s) of the CoC and or the designee of that agency.

XII. Agreement

I have read the aforementioned Agency Agreement and waiver for use of technology of the LA/OC HMIS, Equipment and Services *(if applicable),* and thoroughly understand that this technology is for LA/OC HMIS purposes only.

This Agreement is executed between (agency name) and (continuum name) and upon execution the Agency will be given access to the HMIS. This agreement will be signed by the Executive Director at the Participating Agency.

Executive Director's Name (Print)	Continuum Representative's Name (Print)
Executive Director's Signature	Continuum Representative's Signature
Agency Name	Continuum Name
Date of Signature	Date of Signature

Appendix B: HMIS User Agreement

Los Angeles/Orange County
Homeless Management Information System (HMIS) Collaborative

HMIS User Agreement

I. Purpose

The LA/OC HMIS Collaborative recognizes the priority of client needs in the design and management of the LA/OC HMIS. These needs include both the need to continually improve the quality of homeless and housing services with the goal of eliminating homelessness in the Los Angeles and Orange County regions, and the need to vigilantly maintain client confidentiality, treating the personal data of our most vulnerable populations with respect and care.

As the guardians entrusted with this personal data, HMIS Users have a moral and a legal obligation to ensure that the data they collect is being collected, accessed, and used appropriately. It is also the responsibility of each user to ensure that client data is only used to the ends to which it was collected, the ends that have been made explicit to clients and are consistent with the mission of the LA/OC HMIS Collaborative, *to use HMIS to advance the provision of quality services for homeless person, improve data collection, and promote more responsive policies to end homelessness in Los Angeles and Orange Counties.* Proper user training, adherence to the LA/OC HMIS Collaborative Policies and Procedures, and a clear understanding of client confidentiality and HMIS user responsibility are vital to achieving these goals.

II. Relevant points regarding Client Confidentiality

- A client consent form must be signed by each client whose data is to be entered into the LA/OC HMIS.
- Client consent may be revoked by that client at any time through a written notice.
- No client may be denied services for failure to provide consent for LA/OC HMIS data collection.
- Clients have a right to inspect, copy and request changes in their LA/OC HMIS records.
- HMIS Users may not share client data with individuals or agencies that have not entered into an HMIS Agency Agreement with the LA/OC HMIS Collaborative and obtained written permission from that client.
- Excluding information shared in the client profile, HMIS users may not share client data with any connecting agency that is not specified in their agencies interagency, data shared form without obtaining a written permission from the client.
- HMIS Users will maintain LA/OC HMIS data in such a way as to protect against revealing the identity of clients to unauthorized agencies, individuals or entities.
- Personal User Identification (User ID) and Passwords must be kept secure and are not to be shared.
- Confidential information obtained from the LA/OC HMIS is to remain confidential, even if my relationship with (Agency Name) changes or concludes for any reason.
- Misrepresentation of the client data by entering known, inaccurate information is prohibited. Any information that is not given by the client should be mark unknown.
- Discriminatory comments based on race, color, religion, national origin, ancestry, handicap, age, sex and sexual orientation are not permitted in the LA/OC HMIS. Profanity and offensive language are not permitted in the LA/OC HMIS.
- The LA/OC HMIS is to be used for business purposes only. Transmission of material in violation of any Federal or California State regulations or laws is prohibited and includes material that is copyrighted, and/or legally judged to be threatening or obscene. LA/OC HMIS will not be used to defraud the Federal, State, or local government or an individual entity or to conduct any illegal activity.
- Any HMIS User found to be in violation of the LA/OC HMIS collaborative Policies and Procedures, or the points of client confidentiality in this User Agreement, will result in immediate suspension of your access to the LA/OC HMIS and may jeopardize your employment status with (Agency Name).

III. User Responsibilities

I affirm the following:

1. I have received training in how to use the LA/OC HMIS.
2. I have read and will abide by all policies and procedures in the LA/OC HMIS Collaborative Policies and Procedures Manual.
3. I will maintain the confidentiality of client data in the LA/OC HMIS as outlined above and in the LA/OC HMIS collaborative Policies and Procedures Manual.
4. I will only collect, enter and extract data in the LA/OC HMIS relevant to the delivery of services to people in housing crisis in Los Angeles and Orange County region.
5. I understand that my User ID and Password are for my use only and must not be shared with anyone.
6. I agree to take all reasonable precautions in keeping my password physically secure.
7. I agree to use the data within the LA/OC HMIS only for the purposes of homeless service delivery.
8. I agree to refrain from leaving my computer unattended while logged into the system and further agree to log out of the system before leaving my work area.
9. I agree to properly protect and store in a secure location client specific hardcopy information printed from the LA/OC HMIS.
10. I agree to notify my Agency Administrator and HMIS System Administrator in the case where I suspect that LA/OC HMIS security has been compromised.
11. I agree, to the best of my ability, to enter and maintain accurate information into the LA/OC HMIS.

Failure to comply with the provisions of this User Agreement is grounds for immediate termination of access to the LA/OC HMIS. The signature below indicates an agreement to comply with the client confidentiality and user responsibilities. There is no expiration date of this agreement.

Agency Name

User First and Last Name (Print)

User Signature Date Signed

Agency Administrator First and Last Name (Print)

Agency Administrator Signature Date Signed

I have read the aforementioned consent and waiver for data entry into the LA/OC HMIS and thoroughly understand that this technology is for LA/OC HMIS purposes only.

Appendix C: Client Consent and Information Release

Orange County Continuum of Care
Homeless Management Information System (HMIS)

Client Consent and Information Release

I. General Client Confidentiality:

The Homeless Management Information System (HMIS) will gather and maintain data to: (a) provide individual case management; (b) produce reports regarding utilization of services; (c) track individual program outcomes; (d) provide accountability for individuals and entities that provide funds for use in the LA/OC region; (e) identify unfilled service needs and plan for the provision of new services; (f) allocate resources among agencies engaged in the provision of services in and around Los Angeles and Orange County region; and (g) be used for all other purposes deemed appropriate by the Los Angeles/Orange County Regional Homeless Management Information System (HMIS) Collaborative.
Generally, an agency may not disclose any information contained within this system which could identify a client unless:

1. The client consents in writing;
2. The disclosure is allowed by a court order; or
3. The disclosure is made to medical personnel in a medical emergency or to qualified personnel for research audit or program evaluation.

Federal law and regulations do not protect any information about a crime committed by a client either at the shelter or against any person who works for the shelter or about any threat to commit such a crime.

Federal laws and regulations do not protect any information about suspected child abuse or neglect from being reported under state law to appropriate state or local authorities. (See 42 USC 290dd-3 and 42 USC 290ee-3 for federal laws and 42CFR Part 2 for federal regulations.)

_____ **(Please initial)** I understand and acknowledge that the data pertaining to the services provided to me by the Agency and the records maintained by the Agency may include medical/health information and other information, the privacy of which may be protected by federal and or California law, and expressly consent to the release of such information as well as the information expressed in the sections above regarding crimes and child abuse/neglect.

II. The LA/OC HMIS:

The LA/OC HMIS is an electronic, web-enabled database used to store information about clients utilizing housing and homelessness services in the Los Angeles County. Within the Los Angeles/Orange County HMIS Regional Collaborative, there are four separate Continua of Care including: the Los Angeles Homeless Service Authority (LAHSA), the Orange County Continuum of Care, the City of Glendale and the City of Pasadena. HMIS data for each continuum resides in a secure database containing data from agencies within their respective continuum. As a general rule, data sharing will be initially limited to participating agencies within a particular continuum. However, with client consent, data may be shared within the LA/OC Regional HMIS to avoid duplicative client intakes. The LA/OC Regional HMIS Collaborative reserves the right, at a later date, to expand data sharing to include collaborative wide data. This database enhances the delivery of client services by providing the ability for program staff to electronically track individual cases over time. The LA/OC Regional HMIS is also used to produce aggregate reports that can be used to track program outcomes, provide accountability for program funders, identify unfilled service needs, and plan for new service provision.

All agencies, which have been granted access to the LA/OC HMIS, have agreed to abide by all laws, and the

LA/OC HMIS Policies and Procedures pertaining to client confidentiality and user conduct. Individual client data is available through the LA/OC Regional HMIS to non-custodial agencies.

III. Inter-Agency Client Intake Data Sharing:

Basic client profile data, which includes client intake information, may be shared with agencies participating in the LA/OC HMIS in an effort to reduce the event of duplicative client intakes. The information that may be shared includes client and household demographics, education and employment history, photo identification and other related documents. No individual client data will be shared outside of the LA HMIS or with any LA/OC Regional HMIS user without explicit client permission.

Individual client data and program and service data will be shared with all agencies within the LA/OC HMIS who have signed an Inter-Agency Data Sharing Memorandum of Agreement.

IV. Client Rights and Consent:

- ✓ By signing below, I understand and acknowledge that, based on agency policy, I have the right to: (a) inspect, copy, and request amendment of records maintained by the Agency related to the provision of services to me and to receive a paper copy of this form; (b) request restriction of how my data, information and records are utilized and disclosed but that the Agency is not required to agree to such requested restrictions; (c) request that the Agency communicate with me about my services in a manner designed to promote confidential communications; and (d) if I believe my privacy rights have been violated I may file a grievance with the Agency or the LA/OC HMIS by providing written notice of the alleged violation. I understand I will not be retaliated against for filing such a complaint.

- ✓ By signing below, I also understand and acknowledge that I have the right to opt out of having my data, information and records shared with the LA/OC HMIS and other affiliated agencies upon written notice to the Agency. I understand I have the right to not answer any questions unless entry into the Agency's program requires it. I further understand and acknowledge that I may revoke this consent at any time upon written notice to the Agency. However, I understand and acknowledge that regardless of my decision to opt out or revoke consent; my data may be disclosed to the LA/OC HMIS and included in an aggregated and de-identified form for purposes of making future policy and program decisions.

- ✓ By signing below I consent to the collection LA/OC HMIS data pertaining to my participation in this shelter program. I understand that data pertaining to my shelter stay may be used for case management as well as research and evaluation, and I am entitled to the results of any such research or evaluation reports.

  I understand that I am entitled to services even if I choose not to consent to data sharing subject to the agency's specific program requirements.

_____ **(Please initial)** I understand and acknowledge that the Agency is required to abide by the terms of this notice but that the Agency reserves the right to change the terms of this notice and to make such revised or changed notice effective for information already held by the Agency as well as information received in the future.

_____ _____

SIGNATURE OF CLIENT or GUARDIAN **DATE**

_____ _____

SIGNATURE OF AGENCY WITNESS **DATE**

Appendix D: Privacy Notice

Los Angeles/Orange County
Homeless Management Information System (HMIS) Collaborative

PRIVACY NOTICE

THIS NOTICE DESCRIBES HOW INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION.

PLEASE READ IT CAREFULLY.

Effective Date: _____

Our Duty to Safeguard Your Protected Information

(Agency Name Here) collects information about who uses our services. We will ask for your permission to enter the information we collect about you and your family into a computer program called the LA/OC HMIS. Although the LA/OC HMIS helps us to keep track of your information, individually identifiable information about you is considered "Protected Information". We are required to protect the privacy of your identifying information and to give you notice about how, when and why we may use or disclose and information you may give us.

We are also required to follow the privacy practices described in this Notice, although **(Agency Name Here) reserves the right to change our privacy practices and the terms of this Notice at any time.** You may request a copy of the notice from any participating **LA/OC HMIS Collaborative Agency**.

How We May Use and Disclose Your Information

We use and disclose collective information for a variety of reports. We have a limited right to include some of your information for reports on homelessness and services needed by those who are homeless. Information that could be used to tell who you are will never be used for these reports. We will not turn your information over to a national database. We must have your written consent to use or disclose your information unless the law permits or requires us to make the use or disclosure without your permission. **Please review the Client Consent/Release of Information Authorization for details. You must sign this form before we can use your information, but you do not have to sign the form in order to receive services.**

Your Rights Regarding Your Information

- ✓ You have the right to get services even if you choose **NOT** to participate in LA/OC HMIS. However, clients may be refused program entry for not meeting other agency eligibility criteria.
- ✓ You have the right to ask for information about who has seen your information.
- ✓ You have the right to see your information and change it, if it is not correct.

Appendix E: Mandatory Collection Notice

LOS ANGELES/ORANGE COUNTY
HOMELESS MANAGEMENT INFORMATION SYSTEM (HMIS)
MANDATORY COLLECTION NOTICE

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 as mandated by law or as requested from organizations that fund this program. Other personal information we collect is necessary to operate programs, improve services and better understand the needs of homelessness. We collect appropriate information only.

A Privacy Notice is available upon request.

Appendix F: Client Revocation of Consent to Release Information

Los Angeles/Orange County
Homeless Management Information System (HMIS)

Client Revocation of Consent to Release Information

I, _____ hereby revoke permission for this agency to share my personal information in the LA/OC HMIS. I understand that my information will remain in LA/OC HMIS as part of the non-identifying data collected on homeless services provided by the Continuum of Care.

I understand that information that has already been entered remains in the system. By canceling my agreement for participation in the LA/OC HMIS my personal information that has been saved will be restricted.

I further understand that any information entered and/or shared under my previously agreed-to consent will continue to be shared and that this Client Revocation of Consent applies to any information entered into the system from this day forward.

I also understand that the disclosure of my non-identifying information may be required in some instances, such as for the reporting of aggregate numbers to LA/OC HMIS Collaborative and to agencies that provide funding to this agency.

LA/OC HMIS and this agency are hereby released from any legal responsibility or liability for the release, use or disclosure of information I authorized previously.

Agency Name: _____

Agency Representative: _____

Phone Number: _____

Client's Full Name: _____

SSN/Client's ID Number: _____

_____ _____
Client Signature Date

Appendix G: Interagency

Los Angeles/Orange County
Homeless Management Information System (HMIS) Collaborative
Interagency Data Sharing Consent Form

Client Name:_____

SSN/Client ID:_____

Date of Birth:_____

Name of Originating Agency:_____

Name of Agency 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

Los Angeles/Orange County
Homeless Management Information System (HMIS) Collaborative

How to File a GRIEVANCE about our Privacy Practices

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 agency. **It is against the law for any agency 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:
(Continuum of Care HMIS)
Attn:
Address, City, State Zip

Date of offense: _____

_____	_____
Name of Individual who violated your privacy rights.	Name of Agency 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 Agency:

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.

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 dismissal from employment or even criminal prosecution.

Agency Name: _____

Printed Name: _____

Signature: _____

Date: _____