LOS ANGELES/ ORANGE COUNTY HOMELESS MANAGEMENT INFORMATION SYSTEM COLLABORATIVE

HOMELESS MANAGEMENT INFORMATION SYSTEM (HMIS) POLICIES AND PROCEDURES

CONTINUUM OF CARE LEAD ENTITIES:
CITY OF GLENDALE
LOS ANGELES HOMELESS SERVICES AUTHORITY
OC PARTNERSHIP
CITY OF PASADENA

Table of Contents

1. PROJECT SUMMARY

A. Background: The Congressional Directive

The Homeless Management Information System (HMIS) refers to a system for tracking the use of homeless programs and producing an unduplicated count of the people using those programs. For FY2001, Congress directed the U.S. Department of Housing and Urban Development (HUD) to ensure that homeless programs using federal funds participate in local systems to track the use of services and housing.[1]

The funding programs include:

- Emergency Shelter Grant (ESG)
- Supportive Housing Program (SHP)
- Shelter Plus Care (S+C)
- Single Room Occupancy Moderate Rehabilitation (SRO Mod Rehab)
- Housing Opportunities for People with AIDS (HOPWA)

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

To follow Congress' directive, HUD has told communities to assess their own needs and select the HMIS software that best meets those needs. HUD has provided substantial technical assistance to the Los Angeles/Orange County HMIS Collaborative to support the planning process.

The LA/OC HMIS is not connected to any federal or national data collection facility and data is not passed electronically to any other national database for homeless or low-income individuals.

B. Organization: The LA/OC HMIS Collaborative

Formed in December 2001, the Los Angeles/Orange County (LA/OC) HMIS Collaborative consists of four Continuum of Care (CoC) Systems in two urban counties:

1. In Los Angeles County, there are three CoCs: The cities of Glendale, and Pasadena each coordinate their own CoC; and the Los Angeles Homeless Services Authority (LAHSA) is responsible for the City of Los Angeles and the balance of Los Angeles County.
2. In Orange County, OC Partnership and its partners Orange County Housing & Community Services Department and Info Link Orange County coordinate the Orange County Continuum of Care.

The basis for this Collaborative is:

- Some homeless service providers have programs in two or more CoCs;
- Homeless persons may travel between CoCs to receive all of the services they need;
- Los Angeles and Orange Counties will benefit from having regional data and reports;
- Los Angeles County, which is divided among three CoC systems, would benefit from having County-wide data and reports;
- Service providers in the two counties could benefit from coordinated planning. This could lead to greater consistency in the information collected and reported, making it easier for agency staff to communicate issues and for clients to understand what agencies are asking.

[1] See HUD Strategy for Homeless Data Collection Conference Report (H.R. Report 106-988), which indicated that "local jurisdictions should be collecting an array of data on homelessness in order to prevent duplicate counting of homeless persons and to analyze their patterns of use of assistance, including how they enter and exit the homeless assistance system and the effectiveness of the systems. HUD is directed to take the lead in working with communities toward this end and to analyze jurisdictional data within three years."

C. Mission Statement & Vision

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

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 experiencing homelessness. Specifically, the HMIS will:

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

D. Software

The LA/OC HMIS Collaborative's goal is to go beyond the HUD mandate of producing unduplicated counts of homeless persons. Our charter is to provide a comprehensive case management system that allows the user to use the collected information to make informed program decisions. Additionally, our selected product includes a focus on Outcomes Management which is intended to provide value by allowing the user to set and measure client and program milestones and target achievements.

The software includes (or will include):

- Outcome Management
- Client demographic data collection
- Comprehensive client case management
- Information and Referral capabilities
- Bed maintenance, tracking and assignment module
- Customized reporting capability
- Customized assessment capability
- Real time data collection and reporting
- Employment, Education and Housing history tracking
- Savings tracking
- Group activities management
- Group case notes management
- Advanced security features
- Outreach capability

2. PARTICIPATION REQUIREMENTS

A. Adherence to Policies

All users and agency representatives must agree to the policies in this document in order to participate in the LA/OC HMIS. A signed agreement to do so is required of all users and Participating Agencies. This section details technical, staffing assignments and training that must be fulfilled prior to being granted access to the system.

The Policies and Procedures manual and all attachments may be amended as needed at any time. Participating Agencies will be notified of any Policies and Procedures manual changes.

B. Participation Agreements

The 2005 Violence Against Women Act (VAWA) Reauthorization Bill restricts domestic provider participation in HMIS. HUD does not require nor expect domestic violence providers to contribute client data directly into the regional HMIS. However, OC Partnership has developed a process whereby domestic violence providers shall on a monthly basis query HMIS to determine whether or not demographic information on their active clients has previously been entered by a non domestic violence provider. In order to do the query the domestic violence provider must do a lookup on, at a minimum, first three characters of the client first name and first four characters of the client's last name, SSN, and DOB. If the agency finds that the client does not exist in HMIS, their information is included in an unidentifiable summary of clients currently in service which captures the following demographic information: age, race and ethnicity, gender, education level, disabled status, veteran status, marital status, primary language, and prior living situation. If the domestic violence provider finds that the client has previously been entered, their information is not included in the summary.

Participating Agencies are those agencies that connect to the LA/OC HMIS for the purposes of data entry, data editing and data reporting. Relationships between the CoC Governing Bodies and Participating Agencies are governed by any standing agency-specific agreements or contracts already in place, the **HMIS Agency Agreement**, and the contents of the Policies and Procedures Manual. All Participating Agencies are required to abide by the policies and procedures outlined in this manual.

Prior to obtaining access to the LA/OC HMIS, every agency must adopt the following documents:

- **HUD Data and Technical Standards**
- **HMIS Agency Agreement** – The agreement made between the Participating Agency Executive Management and the local CoC Governing Body which outlines agency responsibilities regarding their participation in the HMIS. This document is legally binding and encompasses all state and federal laws relating to privacy protections and data sharing of client specific information.
- **Interagency Data Sharing Agreement** – Must be established between agencies if sharing of client level data above and beyond the minimum shared elements (Central Intake) is to take place.
- **Client Consent/Information Release Forms** – May be implemented and monitored by agencies and would require clients to authorize in writing the entering and/or sharing of their personal information electronically with other Participating Agencies throughout the LA/OC HMIS where applicable.
- **HMIS User Agreement** – Signed by each HMIS User, the user will agree to abide by standard operating procedures and ethics of the HMIS.
- **Mandatory Collection Notice** – Each Participating Agency will post a written explanation describing agency's policies regarding mandatory collection of client data to be stored on the HMIS.

- **Privacy Notice** – Each Participating Agency will post a written explanation describing the agency's privacy policies regarding data entered into the LA/OC HMIS.
- **Statement of Client Rights Brochure** – A written explanation of privacy practices and security measures that will be enforced to protect the client's information on the LA/OCHMIS. This statement should be handed to the client at time of entry into the system.
- **Client Revocation of Consent to Release Information Form** – Client revokes permission to share or release personal information in the LA/OC HMIS.
- **Grievance Form** – The client has a right to file with the local CoC Governing Body if the client feels that the Participating Agency has violated their rights.
- If Applicable, **Transfer of Data Agreement** – The agreement made between the Participating Agency Executive Director and the local CoC Governing Body to transfer, upload, or migrate data from the agency's existing system to the LA/OC HMIS.
- **Termination of Employee** – This form is to notify the HMIS System Administrator that the referenced employee will no longer work for the organization and thus all access to the HMIS needs to be removed.

All agencies will be subject to periodic on-site security assessments to validate compliance of the agency's information security protocols and technical standards.

Two additional agreements will be entered into outside the jurisdiction of the Participating Agency. These agreements will be held by the CoC Governing Body:

- **HMIS System Administrator Agreement** – Each HMIS System Administrator will agree to abide by standard operating procedures, confidentiality and ethics of the HMIS.
- **Confidentiality Certification** – The HMIS software vendor's employees will agree to abide by confidentiality and ethics standards as stated in the LA/OC HMIS Policies and Procedures Manual.

C. Technical Standards

Each CoC Governing Body is responsible for each Participating Agency's oversight and adherence to the Technical Standards. Please check with your CoC Governing Body to ensure you are in compliance.

High Speed internet access

- DSL, Cable, T1 Line, etc.
- No dial up connections
- Dedicated IP address is recommended
    - DHCP may be used
    - Static IP address will be required if the administrative burden of using DHCP becomes too great

PC w/ Internet Explorer 5.5 or higher (free)

- No Netscape, Mozilla, AOL etc…
- No Mac's, UNIX, Linux etc…

Microsoft .NET Framework Version 1.1 (free)

- Can be downloaded from www.microsoft.com/downloads.
- Windows 2000, Windows 98, Windows NT sp6a, Windows XP
- If running XP we recommend running SP2

Firewall

- Must use Network Address Translation (NAT) behind firewall
- If wireless is used must be protected with at minimum Wired Equivalent Privacy (WEP)
- Must be placed between any internet connection and PC for the entire network.

Antivirus on ALL systems connected to an agency's network

- Must have most recent Virus Security Updates
- This includes systems which Terminal or VPN into the network

D. Staffing Responsibilities

Each Participating Agency will need to have staff to fulfill the following roles. The responsibilities assigned to these individuals will vary. However, all functions must be assigned and communicated to the HMIS System Administrator(s).

Role	Functions
Executive Management *Oversight Responsibility for all activities associated with agency's participation in the LA/OC HMIS.*	• Signs the **HMIS Agency Agreement** and any other required forms prior to accessing the LA/OC HMIS • Authorizes data access to agency staff and assigns responsibility for custody of the data. • Establishes, adopts and enforces business controls and agrees to ensure organizational adherence to the LA/OC HMIS Collaborative Policies and Procedures. • Communicates control and protection requirements to HMIS Users and other agency staff as required. • Assumes responsibility for the integrity and protection of client-level data entered into the system. • Assumes liability for any misuse of the software by agency staff. • Assumes responsibility for posting **Privacy Notice** and **Mandatory Collection Notice**. • Assumes the responsibility for the maintenance and disposal of on-site computer equipment. • Provides written permission to the HMIS System Administrator to perform the decryption of data to upgrade LA/OC HMIS technology. • Provides written permission to the HMIS System Administrator to perform the decryption of agency data to upgrade the LA/OC HMIS database server to new technology when the database becomes obsolete. • Periodically reviews system access control decisions.

Role	Functions
Outcome Manager *Internal agency resource for outcome management planning and implementation*	• Serves as the liaison between agency managers, HMIS Users and Outcome Specialists. • Attends required Outcome Manager training, Agency Administrator training, and technical assistance (TA) sessions. • Develops and enters into the LA/OC HMIS the outcome performance targets and milestones. • Reports system problems and data-related inconsistencies to HMIS System Administrator or Outcome Specialist as needed.
Agency Administrator *Technical Liaison to the HMIS System Administrator*	• Liaisons between HMIS Users and HMIS System Administrators. • Attends required Agency Administrator training. • Provides agency HMIS Users support and clarification on system functionality. • Identifies Agency computers that will have access to the LA/OC HMIS. • Ensures that all authorized persons complete all required steps before obtaining access to the system and adhere to the responsibilities of an HMIS User as outlined in the Policies and Procedures Manual. • Responsible for the distribution, collection, and storage of signed **HMIS User Agreements** and Policies and Procedures Manual acknowledgments. • Identifies and responds to violations of the Policies and Procedures. • Notifies agency users of interruptions in service. • Reports system problems and data-related inconsistencies to HMIS System Administrator. • Ensures the virus protection procedure is enforced at desktop computers, servers, and all other computer systems connected to the network via LAN/WAN and/or remote connections. • Reports to the HMIS System Administrator the staff changes at the Agency.

Role	Functions
HMIS User	• Completes training on the appropriate use of the LA/OC HMIS prior to accessing the system. • Acknowledges an understanding of this Policies and Procedures Manual. • Adheres to any agency policies that affect the security and integrity of client information. • Is responsible for LA/OC HMIS Data Quality. Data quality refers to the timeliness of entry, accuracy and completeness of information collected and reported in HMIS. • Signs **HMIS User Agreement** and any other required forms prior to accessing system. • Reports system problems and data-related inconsistencies to Agency Administrator or Outcome Manager as appropriate. • If applicable, obtains client signature on **Client Consent/Information Release Form**. • Gives client written copy of **Statement of Client Rights Brochure**. • Verbally communicates client's rights and uses of client's data.

E. Training

All HMIS Users must complete training appropriate to their functions as described above prior to gaining access to the LA/OC HMIS.

The CoC will provide training to all users at the beginning of the agency's LA/OC HMIS implementation.

Agency Administrators will be trained to provide basic user follow-up training to support agency staff using the LA/OC HMIS. CoC trainers will provide periodic refresher training for other users as needed.

Identified training tracks include:

- Agency Administrator training
- Outcome Management training
- HMIS User training
- Ethics and Confidentiality training

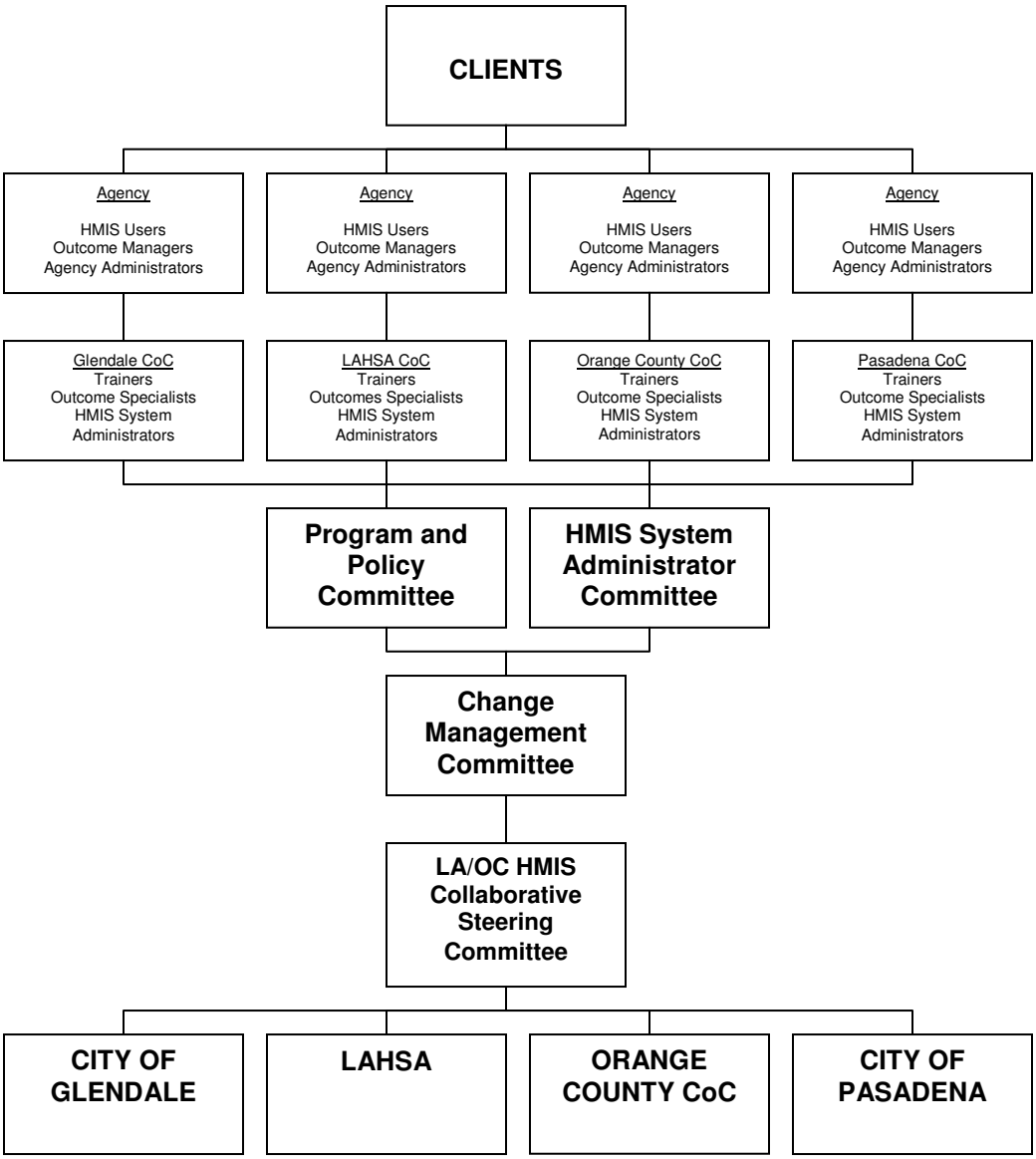
F. Participation Fees

Each Continuum reserves the right to charge a participation fee to use the system. Please consult your CoC Governing Body regarding fees.

3. SYSTEM ROLES AND RESPONSIBILITIES

A. LA/OC HMIS Organization Chart

Definitions of System Roles and Responsibilities are located under Section 10: Terminology.



4. CLIENT RIGHTS

Clients served by agencies participating in the LA/OC HMIS have the following rights:

A. Communication

1. Clients have a right to privacy and confidentiality
2. Clients have a right to not to answer any questions unless entry into the Agency's program requires it.
3. Client information may not be shared without informed consent (posting of **Privacy Notice** and **Mandatory Collection Notice**)
4. Every client has a right to an understandable explanation of the LA/OC HMIS and what "consent to participate" means. The explanation shall include:
    a. Type of information collected
    b. How the information will be used
    c. Under what circumstances the information will be used
    d. That refusal to provide consent to collect information shall not be grounds for refusing entry to the program.
    e. A copy of the consent shall be given to the client upon request, and a signed copy kept on file at the Participating Agency, if applicable.
    f. A copy of the **Privacy Notice** shall be made available upon client request.
    g. A copy of the Statement of Client Rights shall be made available upon client request.

B. Participation Opt Out

Clients have a right not to have their personal identifying information in the LA/OC HMIS shared outside the agency, and services cannot be refused if the client chooses to opt out of participation in the HMIS. However, clients may be refused program entry for not meeting other agency eligibility criteria.

In the event that a client previously gave consent to share information in the LA/OC HMIS and chooses at a later date to revoke consent (either to enter or to share), a **Client Revocation of Consent to Release Information Form** must be completed and kept on file.

C. Access to Records

A client has the right to request access to their personal information stored in the LA/OC HMIS from the authorized agency personnel. The 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.

When requested, a client has the right to:

1. View his or her own data contained within the LA/OC HMIS; or
2. Receive a printed copy of his or her own data contained within the LA/OC HMIS;
3. Access to available audit reports.

No client shall have access to another client's records within the LA/OC HMIS. However, parental/guardian access will be decided based upon existing agency guidelines. The information contained in the Central Intake section of the LA/OC HMIS 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. An agency may not share any information about the client entered by other agencies beyond the Central Intake section.

D. Grievances

The client has the right to file a grievance with an agency. All Participating Agencies must have written grievance procedures that can be provided to a client on demand. If, after following the

grievance procedure, the grievance is not resolved, the complaint may be escalated to the local CoC Governing Body.

5. POLICIES FOR USERS AND AGENCIES

A. User Access

User access will be granted only to those individuals whose job functions require legitimate access to the LA/OC HMIS. Each HMIS User will sign an **HMIS User Agreement** and satisfy all the conditions herein before being granted access to the LA/OC HMIS.

Explanation: The Participating Agency will determine which of their employees need access to the LA/OC HMIS. Identified users must sign the **HMIS User Agreement** stating that he/she has received training, will abide by the LA/OC HMIS Collaborative Policies and Procedures Manual, will appropriately maintain the confidentiality of client data, and will only collect, enter and retrieve data in the LA/OC HMIS relevant to the delivery of services to people in housing crisis in the area served by the LA/OC HMIS Collaborative. The Agency Administrator will be responsible for the distribution, collection and storage of signed **HMIS User Agreements**. The existence of signed **HMIS User Agreements** will be verified and a copy obtained during the onsite review process by the HMIS System Administrator.

B. User Activation

The HMIS System Administrator will provide unique user names and passwords to each Participating Agency user.

Explanation: User names will be unique for each user and will not be shared with other users. The HMIS System Administrator will set up a unique user name and password for each user upon completion of training and receipt of the signed **HMIS User Agreement** and the receipt of the signed acknowledgement of the Policies and Procedures Manual from each user via the Agency Administrator. The sharing of user names will be considered a breach of the **HMIS User Agreement**.

C. Passwords

Passwords must be no less than eight and no more than sixteen characters in length, and must be alphanumeric upper and lower case with special characters. The HMIS System Administrator will communicate passwords directly to the user. Agency Administrators will contact the HMIS System Administrator to reset a user's password.

Forced Password Change (FPC): The FPC will occur every one hundred and eighty (180) consecutive days. Passwords will expire and user will be prompted to enter a new password. Users may not use the same password consecutively, but may use the same password more than once.

Unsuccessful logon: If a User unsuccessfully attempts to logon three times, the User ID will be "locked out", access permission revoked and user will be unable to gain access until their password is reset by the HMIS System Administrator in the manner stated above.

D. User Levels

1. **Client Data Entry:** This group consists of the front line intake workers. They will have access to just the central intake forms in order to intake a client.

2. **Case Manager:** This group consists of case managers who provide the day-to-day updating of client files. Case Managers will have access to all records located in Central Intake and in the Client folder, including Program Entry, Case Notes, Track Savings, Assessments, Group Services, and Program Exit.

3. **Program Manager:** This group has all the access listed above, and additional access to reporting features located in the HMIS.

4. **Agency Administrator:** This group has all the access listed above, and additional access to the Agency Folder, in which they will maintain agency set-up information like program set-up, milestones, targets, and contracts/grants.

5. **Reports Only**: This group includes any user at the agency who does not need to have access to client information except in report form. These reports can be canned (already built) reports, ad-hoc reports, and customized reports.

6. **HMIS System Administrator:** This group of top-level LA/OC HMIS Administrators supports all agencies within the continuum and will have access to every part of the LA/OC HMIS in order to support users.

E. Confidentiality and Informed Consent

All Participating Agencies agree 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 program level client data with written consent by the client, or the client's guardian, unless otherwise provided for in the regulations or laws.

Explanation: Participating Agencies are required to develop procedures for providing oral explanations to clients about the usage of a computerized HMIS and are required to post a **Mandatory Collection Notice** and a **Privacy Notice** in order to share central intake client information with other HMIS Participating Agencies. HUD Data Standards provide guidance for Participating Agencies regarding certain HMIS policies. However, in instances of conflict between state or federal law and the HUD Data Standards, the state and/or federal law take precedence.

Oral Explanation: All clients will be provided an oral explanation stating their information will be entered into a computerized record keeping system. The Participating 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. The explanation must contain the following information, which is also included in the "**Statement of Client Rights Brochure**":

- What LA/OC HMIS is: a web-based information system that homeless service agencies within the LA/OC Region use to capture information about the persons they serve.
- Why gather and maintain data: Data collection supports improved planning and policies including determining whether desired outcomes were achieved and where more or other resources may be needed, identifying best and promising practices, and identifying factors that support or hinder achievement of outcomes.
- Security: only staff who work directly with clients or who have administrative responsibilities can look at, enter, or edit client records.
- Privacy Protection: No program level information will be released to another agency or individual without written consent; client has the right to not answer any question, unless entry into a program requires it; client information is stored encrypted on a central database and information that is transferred over the web is transferred through a secure connection; client has the right to know who has added to, deleted, or edited their LA/OC HMIS record.
- Benefits for clients: facilitates streamlined referrals, coordinated services, unduplicated intakes and access to essential services and housing for clients.

Written Explanation: Each client whose program level information is being shared with another Participating Agency must agree via the **Interagency Data Sharing Agreement**. A client must be informed as to what information is being shared and with whom it is being shared.

- Information Release: The Participating Agency agrees not to release client identifiable information to any other organization pursuant to federal and state law without proper client consent. See attached Client Consent Form and Regulations below.
    - Regulations: The Participating Agency will uphold all relevant Federal and California State Confidentiality regulations to protect client records and privacy. In addition, the Participating Agency will only release client records with written consent by the client, unless otherwise provided for in regulations, specifically, but not limited to, the following:
        - The Participating 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 Participating Agency understands that the Federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patients.
        - The Participating 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.
        - The Participating Agency will abide specifically with the California Government Code 11015.5 regarding program level 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.
- The Participating Agency will not solicit or input information from clients unless it is essential to provide services, or conduct evaluation or research. All client identifiable data is inaccessible to unauthorized users.
- Participating Agencies are bound by all restrictions placed upon the data by the client of any Participating Agency. The Participating Agency shall diligently record in the LA/OC HMIS all restrictions requested. The Participating Agency shall not knowingly enter false or misleading data under any circumstances.
- The Participating Agency shall maintain appropriate documentations of client consent to participate in the LA/OC HMIS.
- If a client withdraws consent for release of information, the Agency remains responsible to ensure that the Client's information is unavailable from date of withdrawal to all other Participating Agencies.
- The Participating Agency shall keep signed copies of the Client Consent Form/Information Release form (if applicable) and/or the **Interagency Data Sharing Agreement** or for the LA/OC HMIS for a minimum of seven years from the date of client exit.
- **Postings: Privacy** and **Mandatory Collection Notice**s must be posted at the agency:
    1. The Agency must post **Privacy** and **Mandatory Collection notice**s at each intake desk or comparable location.
    2. The **Privacy** and **Mandatory Collection notice** must be made available in writing at the client's request.
    3. If the agency maintains an agency website, a link to the **Privacy Notice** must be on the homepage of the agency's website.

F. Data Quality

HMIS Users are responsible for the ensuring LA/OC HMIS Data Quality. Data quality refers to the timeliness, accuracy and completeness of information collected and reported in HMIS. All Participating Agencies agree to enter, at a minimum, the LA/OC HMIS required data elements.

Explanation: Participating Agencies will collect as much relevant client data as possible for the purposes of providing services to that client. The Participating Agency agrees to input the collected data no more one week after date of program entry. The Participating Agency agrees to the data collection commitment by signing the Agency Agreement and is responsible for updating client's records as needed. The HMIS System Administrators will randomly check for data integrity. Any patterns of error (including blank entries) will be reported to the Agency Administrator. When patterns of error have been discovered, users will be required to correct data entry errors and processes. Verification by the HMIS System Administrators will occur to ensure the successful correction of data entry errors and processes. Users may be required to attend additional training as needed.

- The Participating Agency shall only enter individuals in the LA/OC HMIS that exist as Clients under the Agency's jurisdiction. The Participating Agency **shall not** misrepresent its Client base in the LA/OC HMIS by entering known inaccurate information.
- The Participating Agency **will not** alter information in the LA/OC HMIS that is entered by another Agency with known inaccurate information.
- The Participating Agency shall not include profanity or offensive language in the LA/OC HMIS.
- The Participating Agency shall utilize the LA/OC HMIS for business purposes only.
- The transmission of material in violation of any federal or California State regulations is **prohibited**. This includes, but is not limited to, copyright material, material legally judged to be threatening or obscene, and material considered protected by trade secrets.
- The Participating Agency **shall not** use the LA/OC HMIS with intent to defraud federal, state or local governments, individuals or entities, or to conduct any illegal activity.

G. Data Use by LA/OC HMIS Collaborative

Each of the continuums within the LA/OC HMIS Collaborative shall have access to their respective agencies' client data contained within the LA/OC HMIS.

Explanation: For the purposes of system administration, user support, and program compliance, LA/OC HMIS Collaborative will use the data contained within the LA/OC HMIS for analytical purposes only and will not disseminate client-level data. Each continuum may release **aggregate** data contained within the LA/OC HMIS for research and regional reporting purposes only. The System Administrator Agreement must be signed by all HMIS System Administrators.

H. Data Use by Vendor

The Vendor and its authorized subcontractor(s) shall not use or disseminate data contained within the LA/OC HMIS without express written permission.

Explanation: To enforce information security protocols and to ensure that LA/OC HMIS data is used only with explicit permission and if permission is granted, will only be used in the context of interpreting data for research and for system troubleshooting purposes, the Service and License Agreement signed individually by each CoC and the software vendor contains language that prohibits access to LA/OC HMIS data except under the conditions noted above.

I. Data Use by Agency

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

Explanation: As the guardians entrusted with client personal data, HMIS Users have a moral and a legal obligation to ensure that the data they collect is being gathered, 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, ends that have been made explicit to clients and are consistent with the mission of the agency and the HMIS Collaborative to assist families and individuals to resolve their housing crisis. Proper user training, adherence to the LA/OC HMIS Policies and Procedures Manual, and a clear understanding of client confidentiality are vital to achieving these goals. All HMIS Users will sign an **HMIS User Agreement** before being given access to the system. Any individual or Participating Agency misusing, or attempting to misuse the LA/OC HMIS data can be denied. Sanctions exist if users violate any laws related to client confidentiality, as outlined in Section 8: Violations.

J. Maintenance of Onsite Computer Equipment

Participating Agencies commit to a reasonable program of data and equipment maintenance in order to sustain an efficient level of system operation. Participating Agencies must meet the technical standards for minimum computer equipment configuration; Internet connectivity, antivirus and firewall.

Explanation: The Executive Management or designee will be responsible for the maintenance and disposal of on-site computer equipment and data used for participation in the LA/OC HMIS including the following:

1. Computer Equipment: The Participating Agency is responsible for maintenance of onsite computer equipment. This includes the following:
   - Purchase of and upgrades to all existing and new computer equipment for utilization in the LA/OC HMIS.
   - Workstation(s) accessing the LA/OC HMIS must have a username/password to log onto Microsoft Windows Operating System.
   - Workstation(s) accessing the LA/OC HMIS must have locking, password-protected screen saver
   - Workstation(s) accessing the LA/OC HMIS must have a PKI (Public Key Infrastructure) certificate
   - Workstation(s) accessing the LA/OC HMIS 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. Data Storage: The Participating Agency agrees to only download and store data in a secure environment. Refer to Section 2.C: Technical Standards for more information.
3. Data Disposal: The Participating Agency agrees to dispose of documents that contain identifiable client level data by shredding paper records, deleting any information from diskette before disposal, and deleting any copies of client level data from the hard drive of any machine before transfer or disposal of property.

K. Downloading of Data

HMIS 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. HMIS Users may not electronically transmit unencrypted client data across a public network.

Explanation: To ensure that the LA/OC HMIS is a confidential and secure environment, 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. Security questions can be addressed to the HMIS System Administrator. Any personally identifiable information will not be distributed through email.

L. Data Sharing

Basic client information within the system will be shared based upon the level of consent designated by the client within the LA/OC HMIS. A client may choose to limit the period of time for which their data will be shared.

Explanation: Data sharing refers to the sharing of information between Participating Agencies for the coordination of case management and client service delivery. Basic client information in the Central Intake includes:

- Demographics
- Household
- Referral
- Eligibility
- Education/Employment
- Documents

Clients have the ability to agree to the level of consent and time period to which the consent is valid. Participating Agencies are not required to agree to such requested restrictions if collection and sharing of such data is necessary for service delivery and reporting or to consent that is broader than that normally extended at their agency. Clients may elect to share additional information as indicated on the **Interagency Data Sharing Agreement**.

Program level information in either electronic or paper form will never be shared outside of originating agency without written client consent. Information that is shared with written consent will only be used for the purpose of service delivery.

M. Data Release

Aggregate level (client de-identified) data may be released by Agencies, the local Continuum of Care and/or by the LA/OC HMIS Collaborative under certain criteria. Client-level data may only be released by written consent from the client for a specified purpose.

Explanation: Data release refers to the dissemination of aggregate and/or client-level information for statistical, analytical, reporting, advocacy, regional needs assessment, trend analysis, etc.

1. **Agency Release:** Each Participating Agency owns all data it enters into the LA/OC HMIS. The agency may not release any client level information without the express written consent of the client. Agencies may release program and/or aggregate level data for all clients to whom the agency provided services. No individual client data will be provided to any group or individual that is neither the Participating Agency that entered the data nor the client without proper authorization or consent by the client. This consent includes the express written authorization for each individual or group requiring access to the client's data.

2. **Continuum of Care Release:** Each Continuum of Care (CoC) may release **aggregate** information about their own Continuum at the program, sub-regional and regional level. Continuum level aggregate data may be released without agency permission at the discretion of the agency's continuum. The LA/OC HMIS Collaborative will not release agency- or client-specific data to outside groups or individuals.

3. **LA/OC HMIS Collaborative Release:** The LA/OC HMIS Collaborative will develop an annual release of aggregate data in a summary report format, which will be the standard response for all requests for collaborative data. The LA/OC HMIS Collaborative will not release agency- or client- specific data to outside groups or individuals.

N. Agency Customization

A Participating Agency will have the ability to request system customization at the Agency level to reflect the data collection needs for their specific program(s). The LA/OC HMIS contains certain fields that can be tailored at no cost to the agency. Additional customization as performed by the software vendor or Continuum's HMIS System Administrators may be purchased at the expense of the agency.

Explanation: Participating Agencies have some ability to customize LA/OC HMIS fields to meet the specific needs of their program at the discretion of each individual Continuum. At the request of the Agency Administrator, the HMIS System Administrator will evaluate the request and implement the changes as warranted.

O. Offsite Use

Participating Agencies agree to enforce the location access privileges to the LA/OC HMIS. In the future and at the discretion of the LA/OC HMIS Collaborative, a policy that allows only authorized computers to be able to access the LA/OC HMIS from authorized locations through the use of dedicated IP address may be enacted.

Explanation: Access to the LA/OC HMIS may only be allowed from computers specifically identified by the Agency Administrator of the Participating Agency. Those designated computers will be registered electronically with their respective HMIS System Administrator.

Laptops will be held to the same policies and procedures as desktop computers.

P. Technical Assistance regarding Outcomes Management

Technical Assistance led by a designated Outcome Specialist is required for agencies to participate in the LA/OC HMIS.

Explanation: All agencies are required to develop performance targets and milestones and input the data for each program to be entered into the LA/OC HMIS.

Q. Information & Referral Module (I & R)

The I & R Module will be addressed at a later date. Amendments to the Policies and Procedures manual will occur at that time. Potential elements include:

- Sharing of I & R data
- Who has access to I & R data
- Purposes for which I & R data is to be used
- Printing I & R data
- Changes to agency's I & R records

6. TECHNICAL SUPPORT AND SYSTEM AVAILABILITY

A. Technical Support

Each continuum within the LA/OC HMIS Collaborative will provide technical support to all Agency Administrators and HMIS Users as needed.

Explanation: The Agency Administrator will provide first level technical support. Additionally, each Continuum's HMIS System Administration team will provide technical support to Agency Administrators and HMIS Users within their respective continuum.

Technical Support Hours – 9:00 a.m. – 5:00 p.m. (PST), Monday through Friday (Excluding Holidays).

On-call staff will respond in a timely manner to any requests for support made during the above hours. For technical support, please contact:

OC Partnership at (714) 288-4007

Assistance will be provided in the following areas:

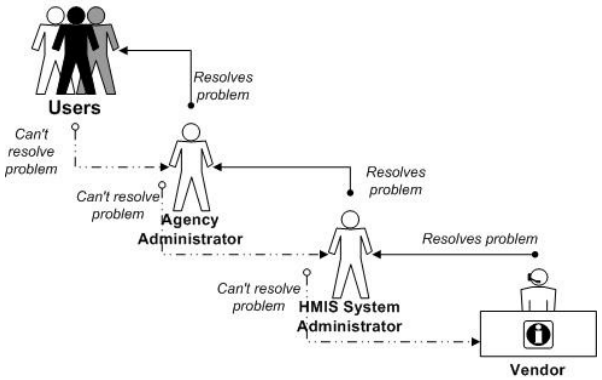
- **Help Desk Support:** Help Desk support is provided to help HMIS Users access and utilize the LA/OC HMIS. Non-LA/OC HMIS related issues will not be supported through the Help Desk (i.e.: frozen monitors, hardware or local connectivity issues, etc.) If the problem is deemed non-LA/OC HMIS related, please contact your agency technical support person.
- **Trainings:** Agency Administrator training, User training, and Outcome Management training & technical assistance.
- **System Customization:** The LA/OC HMIS contains certain fields that can be tailored at no cost to the agency.
- **Reporting:** Training and technical assistance in accessing standardized reports and the creation of ad hoc (custom reports).
- **Data Analysis**: Interpreting reports.

Additional costs may apply in the following areas:

- **System Customization:** Agency-specific customization requests.
- **Reporting:** Agency-specific customized reports.
- **Data Conversion/Migration**: Assist in the development of a data conversion/migration plan, and provide support in data conversion/migration implementation.
- **Data Analysis**: Extensive analysis of agency's data.

Requests should be delineated as follows:

Technical Assistance Flow Chart



B. System Availability and Scheduled Maintenance

The LA/OC HMIS will be available to users at a minimum of 97.5% of the year.

Explanation: Necessary downtime for LA/OC HMIS upgrades and patches will be communicated by HMIS System Administrators system-wide and performed in the late hours when possible. Notification will be made via e-mail and/or fax with the schedule for the interruption to service. The notice will explain the need for the interruption and expected benefits or consequences.

C. Unplanned Interruption to Service

In the event of unplanned interruption to service, HMIS System Administrators will notify all Participating Agencies as soon as possible.

Explanation: When an event occurs that makes the LA/OC HMIS inaccessible, the HMIS System Administrator will analyze and determine the problem. In the event it is determined that the LA/OC HMIS accessibility is disabled system-wide, then the HMIS System Administrators will work with the software vendor to repair the problem. Within two hours of problem awareness, Participating Agencies will be informed of the estimated system availability. HMIS System Administrators will notify Participating Agencies via e-mail and/or fax when service has resumed.

D. User Guide

Every HMIS User will receive a copy of the client manual.

Explanation: The HMIS System Administrators will distribute the LA/OC HMIS Training Manual(s). The documentation will be provided initially at user training and will be available online. The documents will serve to provide users with information needed to effectively use the software as it pertains to their job function, program and agency.

E. Migration of Existing Data

Data migration from legacy systems is allowed upon approval from the local HMIS System Administrators. Migrated data must be non-duplicated and an exact match to the existing LA/OC HMIS field type. The Participating Agency is responsible for the accuracy, completeness and quality of the migrated data.

Explanation: Data migration (or conversion) is the 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.

The Agency's existing system 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.

Data uploads (transfers) are the 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.

The local 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.

All costs associated with the Transfer of Data will be at the Agency's expense.

If the agency's 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.

7. SYSTEM ARCHITECTURE AND SECURITY

A. Password Management Procedure

An HMIS User must notify the Agency Administrator immediately upon realization that his or her password has been lost, forgotten or made public to others. The Agency Administrator is responsible for notification of password breach to the HMIS System Administrator. Upon notification, the HMIS System Administrator will immediately reset the user's password. A user will not receive an initial password without training.

Explanation: The HMIS System Administrator will reset the user password. The new password will be valid from the time of the reset until the next scheduled password change cycle.

- Password needs to contain alphanumeric, upper and lowercase, and special characters.
- Password timeout after 180 days (after timeout the user is required to provide a new legal password to reset)
- Checks are performed to ensure that users cannot reuse their current password.
- If system is dormant for 20 minutes, user will be forced to log back in
- In addition to user password, a session certificate ID is assigned to each user at login time. All transactions must be authenticated by this ID.
- Access logs maintained for every IP that accesses the LA/OC HMIS
- Scheduled audits are in place to regularly test security systems

B. Encryption Management

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

Explanation: Client's confidential information 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.

C. Virus Protection

Agency Responsibilities: All Participating Agency computers and networks must have up-to-date anti-virus software installed that includes the current DATS.

Explanation: All Participating Agency computers should be protected by anti-virus software. The anti-virus software should be updated regularly to maintain maximum protection from the most recently released viruses. In addition, Agency Administrators should update and install the latest security patches for their operating system which are available from the manufacturer.

Vendor Responsibilities: The vendor will take all necessary precautions to prevent any destructive or malicious program (virus) from being introduced to the LA/OC HMIS. Data and application server will be scanned daily for viruses.

Explanation: The vendor will ensure the following:

- Anti virus software (i.e.: Norton Anti-Virus) & live update scheduled daily
- Real-time virus scan enabled

D. Backup and Recovery Procedures

LA/OC HMIS Collaborative has arranged for regularly scheduled backups of the LA/OC HMIS to prevent the loss of data.

Explanation: Multiple levels of backup and storage will be used for key data and files within the LA/OC HMIS. Backups will provide for the loss of multiple cycles.

A. 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.

B. The vendor's designated hosting company will maintain an off-site replicate system, which includes off-site storage of tapes in fireproof containers. Back-up tapes that are awaiting delivery to an off-site storage location shall be stored in a fireproof container. The vendor's designated hosing company will maintain a one year archive of backups.

C. The vendor's recovery procedures will be undertaken on a best efforts basis to achieve the following response time:
   1. Data Loss – confirmation response and recovery implementation within four (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 four (4) hours and full initiation of recovery procedures within 24 hours of reported disruption by the local HMIS System Administrator.
   3. Disaster – notification within four (4) hours and recovery implementation to fully re-establish operations within five (5) business days. (Checking with Vendor)

E. Hosting

LA/OC HMIS servers will be hosted by an off-site hosting company.

Explanation: The vendor will ensure the following:

- Cisco routers with advanced port blocking including:
- Switches with integrated IP blocking based on routine security audit results
- System Software Integrated Security
- High performance firewall
- Security event monitors in place (60 second polling interval) (Checking with Vendor)
- The hosting center partner is Microsoft Solution Provider and applies security updates at the direction of the HMIS vendor.

F. Offsite Access Privileges

All users are subject to Policy 5. O. regarding off-site use.

Explanation: At the local administrative level each user account can be setup to require a single IP address or multiple addresses in addition to their password to complete a login process. Currently, the system supports one IP address for each user account.

G. Auditing and Monitoring

HMIS System Administrators will maintain accurate logs of relevant changes made to the information contained within the database. HMIS System Administrators will monitor access to all systems that could potentially reveal a violation of information security protocols.

Explanation: The HMIS System Administrators are responsible for tracking the transaction logs associated with the maintenance of the LA/OC HMIS. Within the LA/OC HMIS, an audit trail will track client-related activity. Any time a client page is added, edited, deleted or viewed the LA/OC HMIS may record a transaction.

8. VIOLATIONS

A. Right to Deny Access

Each HMIS System Administrator has the right to deny user access to the LA/OC HMIS if a user within the Continuum has violated any of the policies in this document. Any user suspected of violating a policy may be subject to suspension of user privileges until the violation can be resolved.

Explanation: If deemed necessary for the immediate security and safety of LA/OC HMIS data, the HMIS System Administrator has the right to deny or revoke user access to the LA/OC HMIS within their continuum. The HMIS System Administrators will report to the Participating Agency and the LA/OC HMIS Steering Committee the violation of any security protocols.

B. Reporting a Violation

HMIS Users should report security violations to the Agency Administrator, Outcome Manager, or the local HMIS System Administrator as appropriate.

Explanation: All HMIS Users are obligated to report suspected instances of noncompliance. Users should report security violations to the Agency Administrator or the Outcome Manager. The Agency Administrator or Outcome Manager should report violations to the local HMIS System Administrator. The local HMIS System Administrators will review violations of the auditing policies and recommend corrective and disciplinary actions to the LA/OC HMIS Steering Committee or the local CoC Governing Body, as appropriate.

C. Possible Sanctions

The LA/OC HMIS Steering Committee will investigate all potential violations of any security protocols. The LA/OC HMIS Steering Committee may request that the local CoC Governing Body sanction any user found to be in violation of the security protocols. The Agency and/or user may be sanctioned accordingly.

Sanctions by the local CoC include, but are not limited to:

- A formal letter of reprimand
- Suspension of system privileges
- Revocation of system privileges
- Recommendation of termination of employment
- Referral for criminal prosecution

9. GRIEVANCES

A. Client Grievance Process

Clients will contact the Participating Agency with which they have a grievance for resolution of LA/OC HMIS problems. Participating Agencies will report all client grievances to the local CoC Governing Body.

Explanation: Each Participating Agency is responsible for answering questions and responding to grievances from their own clients regarding the LA/OC HMIS. After client has brought an LA/OC HMIS-related complaint to the Participating Agency, the Participating Agency must have a process to respond to the complaint. The Participating Agency will provide a copy of the LA/OC HMIS Policies and Procedures Manual to the client

The Participating Agency must keep all grievances and responses on file at the agency site. The Participating Agency will send written notice of the grievance and response to the grievance to the local CoC Governing Body. The HMIS System Administrator will record all grievances and report them to the LA/OC HMIS Steering Committee. Appropriate action will be taken as required by the local CoC Governing Body.

Each local CoC has overall responsibility for their local LA/OC HMIS effectiveness and will respond if users and/or Participating Agencies fail to follow the terms set forth in the LA/OC HMIS Policies and Procedures Manual, Agency Agreements, and User Agreement or if a breach of client confidentiality or the intentional misuse of client data occurs.

B. Agency Grievance Process

Participating Agencies will report all agency-generated LA/OC HMIS-related grievances to the local CoC Governing Body. If the grievance is related to a problem with the LA/OC HMIS, it must be reported to the HMIS System Administrator. Corrective action will be taken if system-wide changes are warranted.

Explanation: In order for the LA/OC HMIS to serve as an adequate tool for agencies and provide a more accurate picture of our region's homelessness, any grievances related to problems with the LA/OC HMIS must be addressed by the agency in conjunction with the CoC Governing Body with the goal of affecting systemic change where necessary. The local CoC will report grievance problems to the HMIS System Administrator. If system-wide changes are warranted for a corrective action, it will be forwarded to the Change Management Committee for approval.

10. 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 a 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, the City of Long Beach 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. 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 its local inside network addresses to one or more global outside IP addresses and unmaps 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 who 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 made up 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): is 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.

11. 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: _____