San Joaquin Continuum of Care

Homeless Management Information System Policies and Procedures

Adopted: July 11, 2019

INTRODUCTION

In 2001 Congress directed the U.S. Department of Housing and Urban Development (HUD) to collect unduplicated data on the extent of homelessness at the local level [H.R. Report I 06-988; Senate Report I 04-41 0]; the House Report states: Local jurisdictions are required to collect unduplicated data of homeless persons, and analyze patterns of the use of assistance, including how they enter and exit the homeless assistance programs and the effectiveness of the systems. HUD is directed to assist the local jurisdictions and to assist with the implementation and operation of the HMIS which allows homeless service providers to enter the required data elements for tracking homeless populations and the effectiveness of the homeless programs.

San Joaquin County Continuum of Care (SJCoC) receives an annual grant through the McKinney Vento Act (as amended by HEARTH) to operate the HMIS. The CoC has entered into a Memorandum of Understanding with Central Valley Low Income Housing Corp. (CVLIHC) to act as the HMIS Lead Agency.

This document is the Homelessness Management Information System operating manual for SJCoC which provides standard policies and procedures for Homeless Management Information System (HMIS) implementation for the agency managing the HMIS (known as the HMIS Lead or Lead Agency), San Joaquin Continuum of Care, and Contributing HMIS Organizations (CHOs). It also provides the framework for the ongoing operations of HMIS within SJCoC. In subsequent sections, this document addresses HMIS participation by CHOs, client consent rights, data security policies, monitoring and compliance, training assistance, and data entry guidelines. This document also includes several forms used by the HMIS Lead Agency as appendices.

The HMIS software adopted and used by the SJCoC is provided by the vendor Bitfocus, and is commonly known as Clarity. The access site to Clarity is https://stockton.clarityhs.com/. Bitfocus also provides an on line operations manual for end users available at: http://help.clarityhs.com/.

Bitfocus will maintain all database servers and provide daily backups of all HMIS data. In the event of planned server downtime, the HMIS Lead Agency will inform CHOs with as much advance notice as possible in order to allow them to plan their access patterns accordingly.

The HMIS Administrator will address all requests for HMIS-level data from entities other than Participating Agencies or clients. No individual client data will be provided to any group or individual that is neither the Participating Agency, which entered the data, nor the client without proper authorization or consent.

All requests for data from anyone other than a Participating Agency or client will be directed to the CoC HMIS Administrator. Participating Agencies may share agency data as allowed and described by the Agency Agreement. As part of the HMIS Administrator's regular duties, periodic public reports about homelessness and housing issues Stockton/San Joaquin County Region will be issued. No individually identifiable client data will be reported in any of these reports.

HMIS PARTICIPATION

In order to participate in the HMIS in SJCoC, all CHOs must provide an **Agency Partner Agreement** (Appendix A) and a **Data Sharing Memorandum of Understanding** (MOU) (Appendix B). In addition, participating CHO personnel must receive training by the Lead Agency and sign an **End-User Agreement** (Appendix C). Independent researchers or research agencies requesting access to SJCoC's HMIS must provide a completed Research Access Agreement (Appendix D).

Entering data in HMIS does not require client consent. Data sharing requires client consent. Since the SJCoC has adopted a standard of basic data sharing, consent is required based on the following policy statement.

SJCoC HMIS PRIVACY POLICY AND DATA SHARING POLICY

This section presents the overall HMIS Privacy Policy and Data Sharing Policy. Each CHO must either adopt this policy or have their own Privacy and Data Sharing Policy.

SJCoC's HMIS is a system that uses computers to collect information about homelessness. The reason for HMIS is to track program services provided to persons experiencing homelessness within the SJCoC. The goal is to simplify service delivery to people in need.
The HMIS in SJCoC operates over the internet and uses security protections to keep client information safe. Many service providers within SJCoC use the HMIS, so some client information will be shared with other service providers that provide similar services. This is done to provide services to clients in the most efficient manner possible.

Client consent is required for sharing information entered into HMIS. SJCoC has adopted a tiered approach to client consent.

- Tier I minimum standard applies to Street Outreach and similar projects, Services Only (with no physical location), and Initial Assessment Projects (no physical location or by telephone)
    - Agency should provide verbal information as client found in the Privacy Posting. (Appendix E)

- Tier II minimum standard applies to Emergency Shelters, Transitional Housing, Services Only (with a physical location), and Initial Assessment Projects (with a physical location)

    - Projects must post information regarding their privacy policy in an area easily accessible to clients. If the client is being served over the phone, the agency should read the statement to the client found in the Privacy Posting (Appendix E).

- Tier III minimum standard: All other projects (Homeless Prevention, Rapid Re-housing, Permanent Supportive Housing)
    - Projects much post information regarding their privacy policy and have a form signed by the client informing them of the privacy policy and intent to collect information.

This tiered approach to gathering client consent is consistent with regulations set forth by HUD, please see: Federal Register/ Vol. 69, No. 146 / Friday, July 30, 2004 / Notices.

Clients may cancel their consent to share their information at any given time by written request to the agency entering data. The cancellation will not be applied to records already collected from the client. If clients choose to not give consent, it does not make the client ineligible to receive services unless the client is applying for a project that is required by law or regulation to collect and report certain data.

What Data Are We Sharing

Shared between and editable by all participating organizations:

- Client Profile record: Name, Birth date, Social Security Number, Gender, Race, Ethnicity, Veteran status
- Family members, Family Relationships
- Client Photo

Shared between all participating organizations, based on Data Sharing MOU:

- Program Enrollments: Entry Date, Exit Date, Program Name, Organization Name
- List of services provided
- List of subject of general client notes
- General Client assessment data: income, general health, education, etc.

Limited to the organization that created the record (unless a specific ROI is obtained):

- General Client data: income, general health, disabling conditions, education, etc.
- Sensitive client data, such as: Case Notes, HIV/AIDS, Mental Illness, Domestic Violence assessment, alcohol abuse and substance abuse assessment

How We May Use and Disclose Client Information

We only collect information that is needed for 1) case management, 2) administrative, 3) billing and disclosures, 4) analytical, 5) other purposes as permitted by the client or required by law. We do not use or reveal client information without client written consent, except in certain situations. These situations are when required by our funders or by law, or for specific administrative or research purposes.

- **Case Management:** Agencies may use or give client information for case management purposes to help match services. Unless a client requests that his/her record remain

hidden, personal identifiers will only be given to HMIS participating agencies. Agencies may only give client information with written client consent or other specific waiver.

- **Administrative Uses:** Agencies may use client information to carry out administrative functions internally including but not limited to report, checks, oversight, and management functions.
- **Billing Use:** Agencies may use client information for functions related to payment or reimbursement for services if required by the funder/billing agency.
- **Analytical Use:** Agencies may use client information for internal analysis including but not limited to evaluating program effectiveness, creating an unduplicated database on clients served within the system, understanding local and regional needs and trends in homelessness, and assessing SJCoC's Plan to End Homelessness. Information that could be used to identify the client will never be included in these reports.
- **Required by Law:** Agencies may give client personal information that meets the minimum standard necessary for the immediate purpose to comply with legal requirements. Agencies may only give client information to law enforcement entities in response to appropriate legal requests including subpoena or court order.
- **Other:** Agencies may give client information to an agency authorized by law to receive reports of abuse, neglect, or domestic violence if this agency believes the clients are the victim of such treatment on the circumstance that 1) the disclosure is required by law, 2) the client agrees to this disclosure, 3) this agency believes the disclosure is necessary to prevent serious harm. An agency may give client information if it believes it is necessary to prevent or lessen a serious or imminent threat to the health and safety of an individual or public, and if that information is given to a person reasonably able to prevent or reduce that threat.

Client records are maintained on the HMIS system for a period of seven years from its last modification date after which personally identified information can be removed and the remaining information stored in a de-identified format. If clients have any questions about the use of their personal information or are concerned about client privacy or safety, they should share their questions or concerns with staff. If a client feels that the security or integrity of their information has been violated by an end-user or agency itself, CHOs are required to provide a client with a Grievance Filing Form (Appendix F) and submit it to the Lead Agency. The Lead Agency will investigate each grievance and submit suggested actions to the CHO within 30 days. Clients that submit a grievance filing form will not be retaliated against for filing a complaint. Clients may also ask for a copy and/or an explanation of the privacy policy.

Client Rights

- Clients have the right to get services even if they choose **NOT** to participate in the SJCoC HMIS; this right is limited by the nature of the program.
- Clients have the right to ask who has seen their information.
- Clients have the right to see their information and to change it if it's not correct. Clients must show documentation to do so.

If clients don't want their information shared with a specific agency, it is their responsibility to let their case manager or intake worker know. S/he can then take the proper action to honor their request.

DATA SECURITY POLICIES AND PROCEDURES

General Data Security

- Access to all of central server computing, data communications and sensitive data resources is controlled through user identification and authentication. Users are responsible and accountable for work done under their personal identifiers. Access control violations will be monitored, reported, and resolved.

- No one will have direct access to the San Joaquin County Continuum of Care HMIS database through any means other than Clarity or Bitfocus. Access to client data is controlled using security technology and restrictive access policies. Only individuals authorized to view or edit individual client data will have access to that data.

- The CoC HMIS data center is managed by Bitfocus and is located at ViaWest Data Center in Las Vegas, NV. Data from the application is stored in a central server, housed in a Tier-1 ISP secure cage with redundant temperature control and fire suppression systems. Redundant power supplies and surge protection are used on all servers. Bitfocus provides disaster protection and recovery by periodically (no less than once daily) copying application code and data, PGP encrypting copies, and writing them to removable media. Removable media with encrypted backups are stored in a secure off-site location.

- Bitfocus secures the perimeter of its network. The firewall provides real-time, in-line monitoring, interception, and response to network misuse through broad support for the most common attack intrusion detection signatures. Appropriate action can be taken on packets and traffic flows that violate a security policy or represent malicious network activity.

- Clarity can only be accessed with a valid username and password combination, which is encrypted via SSL for Internet transmission to prevent theft. If a user enters an invalid password three consecutive times, Clarity automatically shuts them out for one day.

- In addition to restricting access to only authorized users, Clarity utilizes a system of multiple access levels. These levels automatically detect the user access level and controls access to appropriate data.

- CHOs must establish procedures to handle client paper records. Issues to be addressed include the following: identifying which staff has access to the client paper records and for what purposes, allowing staff access only to those records of clients with whom they work with or for data entry purposes, how and where client paper records are stored, length of storage and disposal procedure, and the disclosure of information contained in client paper records.

- Clarity automatically tracks and records access to every client record by use, date, and time of access. The CoC Lead Agency will regularly review user access privileges and remove identification codes and passwords from their systems when users no longer require access.

Local Physical Safeguards

- The HMIS Lead Agency and CHOs will take all reasonable, foreseeable and protective actions to physically secure the PPI of clients. These actions are listed below but do not represent an exhaustive list of physical safeguards.
  1. To secure protected personal information when transmitting written communication about clients, all users will use the client unique identifier to refer to the client.
  2. Hard copies of client information or reports with protected personal information will be kept in a locked cabinet or storage area when unattended.
  3. Loose papers or notes with client information not stored in the clients file will be securely destroyed.
  4. The lead organization and CHOs will minimize the visibility of computer/tablet/phone screens used to limit HMIS access to unauthorized individuals.
  5. Documents that contain passwords will be kept physically secure.
  6. The servers that house HMIS information will be kept in a secured and monitored facility.

Local Technical Safeguards

- The HMIS Lead Agency and CHOs will take all reasonable, foreseeable and protective actions to technically secure the protected personal information of clients. These actions are listed below but do not represent an exhaustive list of technical safeguards.
  1. Users will change their passwords at least once annually.
  2. Terminals used to access HMIS will have locking screen savers and will be password protected.
  3. Users will not leave SJCoC HMIS open and running when terminal is unattended.
  4. Users will be automatically logged off after 30 or less minutes of inactivity.
  5. Electronic documents stored outside of a private protected local network that contain protected personal information must be password protected.
  6. All devices accessing HMIS must have regularly updated anti-virus software installed that automatically scans files.

Data Disposal

- The HMIS Lead will annually review PPI associated with clients for data no longer in use. Client records will be maintained on the HMIS system for a period of at least seven years from its last modification date after which, PPI can be removed and the remaining information stored in a de-identified format.

Local HMIS Security Plan

This section includes the SJCoC HMIS Security Plan implementation. Within twelve months of adoption by the SJCoC, all parts of the security plan will be completely implemented across all CHOs in SJCoC. The following steps include administrative safeguards to be implemented by

the Lead Agency and CHOs including the designation of authorized representatives that participate in security monitoring for HUD security compliance.

Administrative Safeguards

- There will be one lead security officer designated within the HMIS Lead Agency. The name and contact information of the current security officer at the Lead Agency can be found on the SJCoC website (http://www.sanjoaquincoc.org/). The lead security officer's responsibilities are as follows:
  1. The lead security officer will provide an annual training and guidance to CHO security officers
  2. At least twice a year the Lead Agency will offer a security specific training for users who need to recertify their annual security training
  3. Work with the HMIS Steering Committee and CoC to develop and implement the security plan and review/update it annually
  4. Keep a current list of the names and contact information for each CHO security officers
  5. Be the primary contact for the CHO's security officer and work with them to resolve security issues
  6. Ensure that CHOs are performing background checks on their security officers
  7. Upon receipt of notification from a CHO to deactivate access for employee/volunteers that no longer need access, the lead HMIS security officer will ensure that the Lead Agency deactivates access within five business days.
- There will be one authorized representative designated at each CHO. The responsibilities of this authorized representative are as follows :
  1. Provide name and contact information to the lead HMIS security officer
  2. Ensure that all other employees in the organization are current in their security training
  3. At least once a year the CHO authorized representative will conduct a review of organization practices, policies and procedures to ensure that they are in compliance with the security plan.
  4. Keep list of active users and notify HMIS when within two business days to deactivate access for employee/volunteers that no longer need access
- Both the Lead and CHOs security officers are responsible for ensuring compliance with applicable security standards. CHOs will perform a background check on designated authorized representatives and any administrative users.
- Prior to being given access to HMIS all users must participate in a basic end user security training for certification in HMIS. The training will be provided by someone at the HMIS Lead Agency (unless authorization from HMIS Lead has been given for training to be offered within the organization) and will include information to safeguard privacy and improve data security. Trainees must complete and return a copy of the HMIS End User Agreement. The HMIS Lead Agency will offer the basic end user training on a regular basis and will make efforts to provide additional training as needed. All users of HMIS will need to participate in training addressing data privacy, security and data quality at least annually. The HMIS Lead Agency will offer annual security training at least twice a year.

Reporting Security Incidents

- A security incident is defined as the act of violating an explicit or implied security policy including but not limited to:
  1. Attempts (either failed or successful) to gain unauthorized access to a system or its data
  2. Unauthorized access to PPI due to misplaced, lost, or otherwise compromised access
  3. The unauthorized use of a system for the processing or storage of data
  4. Unwanted disruption or denial of service
  5. Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent
- If a user notices or suspects a security breach, they must immediately notify the CHO's authorized representative. CHO authorized representatives should report incidents to the Lead Agency security officer in instances 1 through 3 above. In instances 4 and 5, CHO authorized representatives should conduct an internal investigation and, if needed then contact the HMIS lead security officer for further resolution. If the user and the CHO's authorized representative is the same person, then that person will contact the HMIS lead security officer in every case when they notice or suspect a security breach.

Disaster Recovery Plan

- In conjunction with the contract with Bitfocus, the HMIS Lead Agency will follow the disaster recovery plan provided. This plan is attached to the existing contract.

Contracts and Other Arrangements

- The HMIS Lead must retain copies of all contracts and agreements executed as part of the administration and management of HMIS.

TRAINING AND TECHNICAL ASSISTANCE

The HMIS Lead Agency will offer regular training opportunities to all users; training content will depend on the user access role.

The HMIS Lead Agency will provide training in the day-to-day use of the HMIS on a regularly scheduled or as needed basis. Training for typical end users will cover the following topics: creating profiles, project enrollment and exits, entering services, assessments and updates, information and referral, security, reports, and client tracking. Training on any agency-modified fields/screens will be the responsibility of the agency making the modification. The HMIS Lead Agency will also provide training about each user's responsibility to protect client privacy and ensure that basic system security is maintained.

All trainings will take place at HMIS Lead Agency offices or on site as requested by the CHO.

Issues and questions related to the operations and use of the HMIS that cannot be resolved through the Clarity Users Help site will be submitted by users to the HMIS Lead Agency, which serves as the local HMIS Administrator. The goal of the HMIS Lead Agency is to respond to issues within 24 business hours of submission. Depending on the complexity of the issue and/or question it might take longer to resolve the issue.

USERS

- The authorized representative for each agency shall identify all authorized users for the agency and the access role or level for each authorized user.
- All HMIS users regardless of access role must execute a User Agreement
- Users are responsible and accountable for all work done under their personal identifiers.
- HMIS users will be responsible for the accuracy of their data entry
- The HMIS Lead Agency will terminate or modify the rights of an End-user upon termination from, or change in, their current position
- Serious or repeated violation by users of the system may result in the suspension or revocation of an Agency's access.
- Any user found to be in violation of security protocols will be sanctioned accordingly.
- Any Agency that is found to have flagrantly violated security protocols may have their access privileges suspended or revoked

DATA QUALITY AND AGENCY PARTICIPATION

All data entered in HMIS must fulfill three data requirements: data must be timely, complete, and accurate.

Timeliness of Data

To be most useful for reporting, an HMIS should include the most current information on the clients served by participating homeless programs. To ensure the most up-to-date data, information for all projects should be entered within three (3) days from when it is collected.

Data Completeness

To release meaningful information from HMIS, data need to be as complete as possible, i.e. they should contain all required information on all people served in a certain type of program (i.e. emergency shelter) during a specified time period. On the macro level, the goal of achieving adequate HMIS coverage and participation by all local programs is essentially about ensuring that the records are representative of all the clients served by these programs. When individual records or whole programs are missing, it is important to consider whether the characteristics of those served by the missing program are significantly different than those that are included. If a client record is missing, then aggregate reports may not accurately reflect the clients served by the program. Similarly, if an entire program is missing, data from HMIS may not accurately reflect the homeless population in the community.

To ensure the most complete data, 100% of the following universal elements should be entered for at least 90% of all clients. All projects should meet CoC target goals.

	CoC target
Name	99% +/- 1%
Social Security Number	90% +/- 10%
Date of Birth	99% +/- 1%

Race	98% +/- 2%
Ethnicity	98% +/- 2%
Gender	99% +/- 1%
Veteran Status	99% +/- 1%
Disabling Condition	98% +/- 2%
Program entry date	100%
Program exit date	100%
Relationship to Head of Household	100%
Housing Move-in date	100%
Living Situation (at entry)	98% +/- 2%
Destination	
Street outreach	5%
Emergency shelters	
Entry/exit	65% +/- 5%
Night by night	5%
Transitional programs	95% +/- 5%
Homeless Prevention	100%
Rapid Re-housing	95% +/- 5%
Permanent supportive housing	95% +/- 5%

Specific Program data elements may be required based on your funding source(s). Complete, current HUD data standards requirements are available at: https://www.hudexchange.info/resources/documents/HMIS-Data-Standards-Manual.pdf and https://www.hudexchange.info/resources/documents/HMIS-Data-Dictionary.pdf

Data Accuracy (Data Validity)

Information entered into HMIS needs to be valid, i.e. it needs to accurately represent information on the people that enter any of the homeless service programs contributing data to HMIS. Inaccurate data may be intentional or unintentional. In general, false or inaccurate information is worse than incomplete information, since with the latter, it is at least possible to acknowledge the gap. It should be emphasized to clients and staff that it is better to enter "don't know" or "refused" or “data not collected” than to enter information known to be inaccurate. To ensure the most up-to-date and complete data, data entry errors should be corrected as soon as identified.

Agency Participation Requirements

- All agencies or projects required to enter data in an HMIS as a condition of receiving funding are considered mandatory reporting entities.
- Agencies or projects not required to enter HMIS data as a condition of funding are considered voluntary reporting entities.
- Connection to the Internet is the sole responsibility of each participating CHO and is a requirement to participate in the SJCoC HMIS.
- Equipment costs for devices related to accessing the SJCoC HMIS are the responsibility of each participating CHO.

- Agencies that are inactive with client entry for more than 30 days may have access deactivated; reactivation will require a written statement of intent of continued participation.
- Once a new agency or new agency project has been added to the HMIS, live data entry must begin within thirty days.

HMIS Participation Costs

- As a general policy the SJCoC has endeavored to make HMIS access for mandatory reporting entities available at no cost for user licenses, training, administration, and related matters. Recognizing that maintaining a robust and effective HMIS is a critical element for the SJCoC, there is recognition that all entities may be required to share the cost. Should that be deemed necessary by SJCoC, the cost of access to the HMIS will be negotiated by the CoC HMIS and Data Committee with each individual mandatory reporting entity. The cost of access by mandatory reporting entities may be less than that for voluntary reporting entities.
- As a general policy the SJCoC has endeavored to make HMIS access for voluntary reporting entities available at no cost for user licenses, training, administration, and related matters. Recognizing that maintaining a robust and effective HMIS is a critical element for the SJCoC, there is recognition that all entities may be required to share the cost. Should that be deemed necessary by SJCoC, the cost of access to the HMIS will be negotiated by the CoC HMIS and Data Committee with each individual voluntary reporting entity. The cost of access by voluntary reporting entities may be more than that for mandatory reporting entities.

Sanctions

- The overall objective of the SJCoC regarding the HMIS is to encourage participation by as many homeless service providers as possible. At the same time, the SJCoC has the responsibility of assuring that all participating agencies meet the standards established by the HMIS policies and procedures.
- In those instances where agencies/programs do not meet established standards, the first step will be to offer remedial training and assistance. In those instances where an agency/program repeatedly fails to satisfactorily address deficiencies, the HMIS and Data Committee may elect to require that agency/program to pay for the cost of each license, plus an annual fee to cover administration and training.
- In instances where an agency/program permits an egregious breach of security, privacy, or confidentiality, the HMIS and Data Committee may suspend, temporarily or permanently, access to HMIS.

San Joaquin Continuum of Care
Homeless Management Information System

AGENCY PARTICIPATION AGREEMENT

AGENCY NAME:_____

For purpose of this agreement, the Contributing HMIS Organization (CHO) will be referred to as "Participating Agency," the Consumer of Services as the "Client" and the San Joaquin Continuum of Care Homeless Management Information System as "SJCoC HMIS." Clarity is a web-based client information system, used by the SJCoC HMIS to record and track homeless client information. It can also be used for case management, determining utilization of services of participating agencies, and sharing of information on services provided to homeless clients.

I. Clarity Use and Data Entry

A. The Participating Agency shall follow, comply with, and enforce the End User Agreement signed by each HMIS user. .
   1. All Participating Agency users of Clarity are required to have had training by SJCoC HMIS Lead agency in using the Clarity database before they will be allowed to use it.
   2. Participating Agency users shall only enter individuals in the Clarity database that exist as Clients in the Participating Agency's jurisdiction. The Participating Agency shall not misrepresent its Client base in Clarity by entering known, inaccurate information.
   3. The Participating Agency shall use Client information in the Clarity database, as provided to the Participating Agency, to assist the Participating Agency in providing adequate and appropriate services to the Client.
   4. Participating Agency users shall consistently enter information into the Clarity database and will strive for real-time, or close to real-time, data entry.

B. Participating Agency users will not alter information in the Clarity database entered by another Participating Agency with known, inaccurate information.

C. Participating Agency users shall not give or share assigned User ID's or passwords for the Clarity database with any other agency, business, or individual.

D. If this agreement is terminated, SJCoC HMIS Lead Agency will, on request, provide the Participating Agency with a copy of their client data. Copies can be in both digital and hardcopy form.

II. Training and Technical Assistance

A. SJCoC HMIS Lead Agency shall assure the provision of training for the necessary Participating Agency users in the use of Clarity. In addition, training updates will be provided as necessary and reasonable and for changes in the software.

B. SJCoC HMIS Lead Agency will be available for continuing technical support as related to Clarity within budgetary constraints.

C. SJCoC HMIS Lead Agency, through its contract with Bitfocus, shall be responsible for the operation and maintenance of network servers, software, data lines, and any other

network or communication devices at the host site which is necessary for the proper function of Clarity. Each Participating Agency shall provide and maintain its own connection to the internet.

III. Confidentiality

A. The Participating Agency shall uphold all applicable federal and state confidentiality regulations and laws that protect Client records and the Participating Agency shall only release client records with written Consent for Release of Information by the client or when required by law or as required by the SJCoC HMIS policies.
   1. The Participating Agency shall not solicit or input information from Clients into the Clarity database unless it is essential to provide services or conduct evaluation or research.
   2. The Participating Agency shall ensure that all staff, volunteers, and other persons issued a User ID and password from Clarity receives client confidentially training provided by the SJCoC HMIS Lead Agency.

B. The Participating Agency may receive access to Client Data entered by other Participating Agencies. All Participating Agencies are bound by restrictions placed upon the data by the client of any other Participating Agency. The Participating Agency shall record, in the Clarity database, all restrictions requested.

C. The Participating Agency shall maintain the appropriate Client Consent forms in their files.
   1. The Participating Agency shall keep signed copies of the Consent form for Clarity for a period of three years.
   2. If a Client withdraws Consent, the Participating Agency remains responsible to ensure that Client's information is unavailable to all other Partner Participating Agencies.

D. This agreement does not require or imply that services must be contingent upon a Client's participation in the Clarity database. Services should be provided to Clients regardless of Clarity participation provided the Clients would otherwise be eligible for the services.

E. According to HMIS Data and Technical Standards produced by HUD, each agency using the HMIS is required to post a Privacy Notice regarding their Privacy Policy and to make the full Privacy Policy available to clients on request.

IV. Use of Data

A. The Participating Agency's access to data on Clients it does not serve shall be limited to non-identifying and statistical data.

B. The Participating Agency may make aggregate data available to other entities for funding or planning purposes pertaining to providing services to homeless persons. However, such aggregate data shall not directly identify individual Clients.

C. If this agreement is terminated, the SJCoC HMIS and remaining Participating Agencies shall maintain their right to the use of all Client data previously entered by the terminating Participating Agency; this use is subject to any restrictions requested by the Client.

D. SJCoC HMIS will use only unidentified, aggregate Clarity data for homeless policy and planning decisions, in preparing federal, state, or local applications for homelessness

funding, to demonstrate the need for and effectiveness of programs, and to obtain a system-wide view of program utilization in the state.

V. Terms and Conditions

A. No party to this agreement shall assume any additional liability of any kind due to the execution of this agreement or participation in the Clarity system. Each party will remain liable, to the extent provided by law, regarding its own acts and omissions. The parties specifically agree that this agreement is for the benefit of the parties only and this agreement does not create rights for any third party.

B. Neither the SJCoC or the SJCoC HMIS Lead Agency shall be liable to any member Participating Agency for any cessation, delay, or interruption of services, nor for any malfunction of hardware, software, or equipment to the extent that any such event is beyond the reasonable control of SJCoC or the SJCoC HMIS Lead Agency.

C. This agreement shall be in-force until revoked in writing by either party provided funding is available.

Agency _____

Address _____

City _____ State. _____ Zip code_____

_____ _____

Authorized Representative Signature Date

Name of Signatory _____ Title _____

print

Appendix A: Revised 05-02-2019

HOMELESS MANAGEMENT INFORMATION SYSTEM
DATA SHARING
MEMORANDUM OF UNDERSTANDING

This Memorandum of Understanding between **SJCoC HMIS Lead Agency** and _____ outlines what client level information is to be shared by all HMIS participating agencies.

It is understood that all agencies and users will be accountable for following all security and privacy policies. The list below outlines which elements are considered "Shared" or "Not Shared". It is understood that a portion of the Universal Data Elements are shared with all San Joaquin Continuum of Care (SJCoC) HMIS Partnering Agencies globally.

Shared:

SSN	Name	Date of Birth	Gender
Race	Ethnicity	Veteran Status	

May be shared:

Program Name	___ agree	___not shared
Enrollment and exit date	___ agree	___not shared
Service history list	___agree	___not shared
General client notes (subject only)	___agree	___not shared

Not shared (default)

- Service history content and notes
- Prior living situation
- Barriers (Chronic health, HIV/AIDS, Mental Health, Substance Abuse, Domestic Violence, etc.)
- Cash Income (sources and amounts)
- Non cash benefits (sources)
- Health Insurance (sources)
- Case notes (contents)

All partnering agencies understand that clients will have to sign a consent form that demonstrates that they understand and agree to have information shared with another agency that is not normally shared as indicated by the MOU. A hard copy of this consent form will be kept in the client's file at _____.

Agreement:

By signing this document _____ agrees to the terms set by this document and accepts all roles and responsibilities herein, as well as compliance with the SJCoC HMIS Policies and Procedures.

Central Valley Low Income Housing Corp.	_____
HMIS Lead Agency	Partnering agency/program
_____	_____
Lead Agency representative (print)	Authorized representative (print)
_____	_____
Signature/date	Signature/date

San Joaquin Continuum of Care
Homeless Management Information System

END USER AGREEMENT

Covered Homeless Organizations (CHO), also known as Participating Agencies, within the San Joaquin Continuum of Care (SJCoC) Homeless Management Information System (HMIS) shall share information for provision of services to homeless persons through a networked infrastructure that establishes electronic communication among the Participating Agencies.

It is a Client's decision to select which information, if any, entered into the Clarity system shall be shared and with which Partner Agencies. Client Consent shall be in conformance with the current SJCoC HMIS Policies and Procedures. Data necessary for the development of aggregate reports of homeless services, including demographics, services needed, services provided, referrals, client goals, and outcomes should be entered to the greatest extent possible.

The Clarity system is a tool to assist agencies in focusing services and locating alternative resources to help homeless persons. Therefore, agency staff should use the Client information in the Clarity system to target services to the Client's needs

RELEVANT POINTS REGARDING CLIENT CONFIDENTIALITY INCLUDE:

- Client consent may be revoked by that client at any time by a written notice
- No client may be denied services for failure lo provide consent for HMIS data collection
- Clients have a right to inspect copy and request changes in their HMIS records.
- SJCoC HMIS users may not share protected client data with any CHO/Participating Agency without obtaining written permission from the client except as allowed by the Data Sharing Memorandum of Understanding.
- The authorized representative of each SJCoC CHO/Participating Agency must notify the SJCoC HMIS Lead Agency upon the termination of employment of any End User.
- Any SJCoC HMIS user found to be in violation of the SJCoC HMIS Policies and Procedures, or the points of client confidentiality in the User Agreement, may be denied access to the SJCoC HMIS Clarity system.

USER RESPONSIBILITY

Your User ID and Password gives you access to the SJCoC HMIS Clarity system. Read and initial each item below to indicate your understanding and acceptance of the proper use of your User ID and password. Failure to uphold the confidentiality standards set forth below is grounds for immediate termination from Clarity.

____I have read and will abide by all policies and procedures in the SJCoC HMIS Policies and Procedures Manual

____ I must take all reasonable means to keep my login and password physically secure.

____ I understand that the only individuals who can view information in Clarity are authorized users and the Clients to whom the information pertains.

____ I may only view, obtain, disclose, or use the database information that is necessary to perform my job.

____ If am logged into Clarity and must leave the work area where the computer is located, I must logoff of Clarity before leaving the work area.

____ A computer that has the Clarity software open and running shall never be left unattended

____ Failure to log off Clarity appropriately may result in a breach in client confidentiality and system security

____ Hard copies of CoC Clarity information must be kept in a locked file

____ When hard copies of CoC Clarity information are no longer needed, they must be properly destroyed to maintain confidentiality.

____ I agree to contact my authorized agency representative for Clarity or the SJCoC HMIS System Administrator in the event I suspect that HMIS security has been compromised.

____ I will only collect, enter, and extract data in the SJCoC HMIS relevant to the delivery of services to people experiencing a crisis in their community.

____ I have received training on the usage of Clarity,

____ I have been made aware of the HMIS Privacy Policy.

____ My electronic device that I use for accessing HMIS has a regularly updated Anti-Virus software and a Spy-ware program,

____ I agree to enter and maintain timely, complete, and accurate information into the HMIS and understand that client data must be protected.

USER CODE OF ETHICS

A. Clarity Users should treat other Participating Agencies with respect, fairness and good faith

B. Clarity Users should maintain high standards of professional conduct in the capacity as a Clarity User.

C. Clarity Users have the responsibility for maintaining and updating client data.

D. Clarity Users have the responsibility to relate to the Clients of other Participating Agencies with full professional consideration.

I understand and agree to comply with all the statements listed above.

User signature: _____

Print Name: _____ Date: _____

Agency Name: _____

Agency Authorized Representative signature: _____

Appendix C: Revised 05-02-2019

Appendix C: Revised 05-02-2019

Homeless Management Information System (HMIS) Agency Privacy Policy Notice

This Notice describes the Privacy Policy of the San Joaquin Continuum of Care (SJCoC) Homeless Management Information System (HMIS). The SJCoC has executed a Memorandum of Understanding with Central Valley Low Income Housing Corp. (CVLIHC) to act as as the HMIS Lead Agency, administering the HMIS on behalf of SJCoC, is governed by the SJCoC Board of Directors

Each CHO (or Participating Agency) is required to adopt this privacy policy related to the use of the SJCoC HMIS. This requirement includes agencies defined as Victim Service Providers and who are required to use a comparable data base. This privacy policy is included as a separate document in Appendix XX.

Not all SJCoC stakeholders have direct access to HMIS. Throughout the SJCoC, there are certain agencies, usually the service provider agencies that are directly interacting with homeless clients, that actively use and contribute to the HMIS. Any agency with access to the HMIS is required to sign an **Agency Partnership Agreement**. All HMIS Lead Agency personnel (including employees, volunteers, affiliates, contractors and associates), and all participating agencies and their personnel, are required to comply with this notice. All personnel in the SJCoC with access to HMIS must receive and acknowledge receipt of a copy of this Notice, agree in writing to comply with it, and receive training on this Privacy Policy before being given access to HMIS.

This Privacy Policy applies to all Personally Identifiable Information that is collected and maintained in the SJCoC HMIS, including electronic and hard copies derived from the HMIS.

Personally Identifying Information, also known as Protected Personal Information (PPI), is defined by the 2004 HUD Data and Technical Standards as: *"Any information maintained by or for a Covered Homeless Organization about a living homeless client or homeless individual that: (1) Identifies, either directly or indirectly, a specific individual; (2) can be manipulated by a reasonably foreseeable method to identify a specific individual; or (3) can be linked with other available information to identify a specific individual."*

The SJCoC HMIS will use only unidentified, aggregate data for homeless policy and planning decisions, in preparing federal, state, or local applications for homelessness funding, to demonstrate the need for and effectiveness of programs, and to obtain a system-wide view of program utilization in the state.

Federal law may require participating agencies to have their own agency-specific privacy policies. Information entered and accessed by the Collaborative may therefore also be covered by additional, agency-specific privacy policies. Participating agencies may be more restrictive in their privacy policies, but may not be less restrictive than this Privacy Policy. In accordance with federal law, all participating agencies are required to post a sign at their intake desks, offices, or website, if applicable, explaining the reasons information is requested.

The SJCoC and the HMIS Lead Agency reserve the right to amend this Privacy Policy at any time. It is possible that an amendment may affect PII that we obtained before the effective date

of the amendment. We will maintain a record of the changes made in amendments and post new versions of this Privacy Policy on the website located at: http://www.sanjoaquincoc.org/

SJCoC has adopted an approach to client consent for use and disclosure of information consistent with regulations set forth by HUD in Federal Register/ Vol. 69, No. 146 / Friday, July 30, 2004 / Notices and with the Coordinated Entry Management and Data Guide (published October 2018) at https://files.hudexchange.info/resources/documents/coordinated-entry-management-and-data-guide.pdf

- "Use" means, with respect to PII, the sharing, employment, application, utilization, examination, or analysis of such information internally within the HMIS participating agency that maintains such information or within the HMIS Lead.
- "Disclosure" means, with respect to PII, the release, sharing, transfer, provision of access to, or divulging of information to an organization outside the HMIS participating agency holding the information or outside the HMIS Lead Agency. Disclosure of any information to any entity that has not signed a Data Sharing MOU and is not required by law can only occur with written client consent

Only information that is needed for 1) coordination of services and case management, 2) administration, 3) billing, and 4) analytics are collected.

- **Coordination of services and case management:** Agencies may use or disclose client information for case management purposes to provide or coordinate services for you and your family to help you end your homelessness. Participating agencies may use or disclose your information to locate suitable services or housing, to conduct referrals and assessments, to determine program eligibility, and to otherwise collaborate to address your specific needs and circumstances.. Unless a client requests that his/her record remain hidden, client PII/PPI will only be shared with an HMIS CHO/Participating Agency that has executed a Data Sharing MOU.
- **Administrative Uses:** Agencies may use client information to carry out administrative functions internally including but not limited to legal, audit, personnel, oversight, and management functions.
- **Billing Use:** Agencies may use client information for functions related to payment or reimbursement for services if required by the funder/billing agency.
- To carry out maintenance and operation of the SJCoC HMIS;
- To create reports for the SJCoC that include your data but only in a manner in which your identity is not disclosed
- **Research Use:** Agencies may use client information for internal analysis including but not limited to evaluating program effectiveness, creating an unduplicated database on clients served within the system, understanding local and regional needs and trends in homelessness, and assessing an agency's progress towards achieving goals and objectives. PII that could be used to identify a client should never be included in these reports. The release of aggregate HMIS data to an entity that is not a CHO/Participating Agency must be approved by the SJCoC Data and HMIS Committee and SJCoC Board of Directors.
- **Required by Law:** Agencies may disclose client personal information that meets the minimum standard necessary for the immediate purpose to comply with legal requirements. Agencies may only disclose client information to law enforcement entities

in response to appropriate legal requests including subpoena or court order. Agencies may disclose client PII to an agency authorized by law to receive reports of abuse, neglect, or domestic violence if this agency believes the clients are the victim of such treatment provided any of the following apply:
1) the disclosure is required by law, such as "mandated reporting"
2) the agency believes the disclosure is necessary to prevent serious harm, or to lessen a serious or imminent threat to the health and safety of an individual or public and the information is given to law enforcement or other person reasonably able to prevent or reduce that threat.

Each CHO must develop and implement a written plan to dispose of or, in the alternative, to remove identifiers from, PII that is not in current use seven years after the PII was created or last changed (unless a statutory, regulatory, contractual, or other requirement mandates longer retention).

Client Rights

- Clients have the right to get services even if they choose **NOT** to participate in the SJCoC HMIS; this right is limited by the nature of the project; some projects are required by law or regulation to collect certain data to establish and document program eligibility.
- Clients have the right to ask who has seen their information.
- Clients have the right to see or receive a copy of their information and to change it if it is not correct. Requests to view or receive a copy of their information shall be in writing and clients must provide proof of identity; the request and proof of identity shall be maintained in the client file (electronic or hard copy). To change information, clients must show documentation verifying the correct information.

If clients do not want their information shared with a specific agency, it is their responsibility to let their case manager or intake worker know, who must then take the proper action to honor that request.

If a client has any questions about the use of their personal information or are concerned about client privacy or safety, they should share their questions or concerns with agency management. If a client feels that the security or integrity of their information has been violated by an end-user or the CHO itself, clients should file a complaint with the Agency, following their procedures that are in place. Clients may also file a complaint with the HMIS Lead Agency; all CHOs/Participating Agencies are required to provide a client with a **Grievance Filing Form** (Appendix F) at their request and submit the completed form to the HMIS Lead Agency; in instances where the HMIS Lead Agency is the subject of a grievance, it will be submitted to the SJCoC Data and HMIS Committee for review and action. The HMIS Lead Agency, in conjunction with the SJCoC Data and HMIS Committee, will investigate each grievance and submit suggested actions to the CHO/Participating Agency within 30 days. Clients that submit a grievance filing form will not be retaliated against for filing a complaint. Clients may also ask for a copy and/or an explanation of the privacy policy.

HOMELESS MANAGEMENT INFORMATION SYSTEM
PRIVACY POSTING

****PLEASE READ CAREFULLY****

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.

If you have any questions or would like to see our privacy policy, our staff will provide you with a copy.

HOMELESS MANAGEMENT INFORMATION SYSTEM
GRIEVANCE FILING FORM

If you think your privacy rights have been violated or you disagree with a decision made about access to your protected information and you have not been able to have the issue resolved by the agency involved, you should complete this form.

****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.****

Your grievance must be submitted in writing to:

Central Valley Low Income Housing Corp.
Attn: HMIS Lead Agency Management
2431 W. March Lane #350
Stockton, CA 95207

You can submit this grievance form by mail to the address above, by faxing it to 209-954-9548, or via email to contact@cvlihc.org .

Please provide information regarding the violation.

Date of offense: _____

Name of **Individual** who violated your privacy rights**:** _____

Name of the **Agency** that violated your privacy rights**:** _____

Provide a description of the grievance:

_____

_____

_____

Please list your contact information:

Name: _____

Phone #: _____

Mailing Address: _____

E-mail: _____

What is the best method to contact you:

____ Phone
____ Mailing Address
____ E-mail

DEFINITIONS/GLOSSARY

Agency: in the context of the HMIS Policies and Procedures, this term can mean a community based 501-c-3 organization or a unit of local government or a sub-division or unit of either type of entity.

Authorized representative: the person designated by a CHO/Participating Agency to execute HMIS related agreements and who is responsible for security and privacy.

Clarity: A web-based information management system used to enter data by homeless service providers within the SJCoC.

Client: An individual about whom a Contributing HMIS Organization (CHO) collects or maintains protected personal information: (1) because the individual is receiving, has received, may receive, or has inquired about services from a CHO; or (2) in order to identify service needs, or to plan or develop appropriate services within the CoC.

CHO - Contributing HMIS Organization: The term used by HUD in the HEARTH Act to describe an organization that enters information related to homeless assistance projects or homelessness prevention projects to a local HMIS; may also be known as a "Participating Agency."

End User (or User): An employee, volunteer, affiliate, associate, and any other individual acting on behalf of a CHO or HMIS Lead Agency who uses or enters data in the HMIS or another administrative database from which data are periodically uploaded to the HMIS.

HMIS - Homeless Management Information System: The information system designated by the CoC to process data in order collect unduplicated counts of individuals and families experiencing homelessness. Through an HMIS, a community should be able to collect information from projects serving homeless families and individuals to use as part of their needs analyses and to establish funding priorities.

ISP: Internet Service Provider

Participating Agency: An agency authorized by the CoC to participate in the HMIS; also known as a Contributing HMIS Organization (CHO).

Personally Identifiable Information (PII): Any information maintained by or for a Covered Homeless Organization about a living homeless client or homeless individual that: (1) Identifies, either directly or indirectly, a specific individual; (2) can be manipulated by a reasonably

foreseeable method to identify a specific individual; or (3) can be linked with other available information to identify a specific individual. May also be known as Personally Protected Information (PPI).

Pretty Good Privacy (PGP): an encryption program that provides cryptographic privacy and authentication for data communication. PGP is used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications.

Protected Health Information (PHI): Any information about the health status, provision of health care that was created or collected by any HIPPA Covered Entity, including health care organizations or providers. Also interpreted as any part of a patient's medical record or payment history.

SJCoC: The San Joaquin Continuum of Care

Universal Data Element (UDE): HMIS Universal Data Elements are elements required to be collected by all projects using the software as an HMIS. Projects funded by any one or more of the federal partners must collect the Universal Data Elements as are projects that are not funded by any federal partner (e.g. missions) but are entering data as part of the Continuum of Care's HMIS implementation.

Universal data elements enable the HMIS the ability to record unique, unduplicated client records, establish participation in a project within a date range, and identify clients who meet time criteria for chronic homelessness.

The Universal Data Elements include:

- 3.1 Name
- 3.2 Social Security Number
- 3.3 Date of Birth
- 3.4 Race
- 3.5 Ethnicity
- 3.6 Gender
- 3.7 Veteran Status
- 3.8 Disabling Condition
- 3.10 Project Start Date
- 3.11 Project Exit Date
- 3.12 Destination
- 3.15 Relationship to Head of Household
- 3.16 Client Location
- 3.20 Housing Move-in Date
- 3.917 Living Situation