San Joaquin Continuum of Care

Homeless Management Information System (HMIS) Policies and Procedures

Adopted: July 11, 2019
Amended: July 14, 2022
Amended: June 8, 2023

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 Homeless Management Information System (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 Continuum of Care's (SJCoC) HMIS is a system to collect information about homelessness. The reason for HMIS is to gather demographic information, track program services provided, and measure program outcomes regarding persons experiencing homelessness within the SJCoC. The goal is to simplify service delivery to people in need and gather data that can help improve systemwide outcomes.

This document provides standard operating policies and procedures for Homeless Management Information System (HMIS) implementation in the San Joaquin Continuum of Care as described in 24 CFR 578 and 576, Notice CPD-17-01, 2017 HMIS Data Standards, and HMIS Privacy and Security Notice. In subsequent sections, this document addresses HMIS participation by Covered Homeless Organizations (CHOs), client consent rights, data security policies, monitoring and compliance, training assistance, and data entry guidelines. A "Covered Homeless Organization" may also be known as a Participating Agency in this document or appendices. This document also includes in the appendices several forms used by the HMIS Lead Agency.

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 online operations manual for end users available at: http://help.clarityhs.com/. The Data and HMIS Committee will conduct an annual evaluation of the HMIS vendor performance and review the HMIS vendor contract for presentation of recommendations to the SJCoC Board of Directors for any changes.

The San Joaquin Continuum of Care, through the Board and Data & HMIS Committee, reserves the right to change or modify the policies and procedures at any time to align with federal requirements or identified needs of the SJCoC. All CHOs/Participating agencies will be notified of any changes in the polies and procedures.

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 within 24 hours of receiving notice in order to allow them to plan their access patterns accordingly.

All data housed in the HMIS is the property of the SJCoC. Participating Agencies have the right solely to the data that they enter. The HMIS Administrator will address all requests for data from entities other than Participating Agencies in accordance with policies recommended by the Data and HMIS Committee and approved by the SJCoC Board. No Personal Identifiable Information (PII) on an individual will be provided to any group or individual that is neither the Participating Agency which entered the data, nor the client, without written authorization or consent except in instances expressly described in these Policies and Procedures or as required by law.

As part of the HMIS Administrator's regular duties, required public reports about homelessness and housing issues throughout the SJCoC will be issued. No PII client data will be reported in any of these reports.

HMIS GOVERNANCE AND STRUCTURE

San Joaquin Continuum of Care (SJCoC) receives an annual grant through the Continuum of Care Program to operate the HMIS. SJCoC has entered into a Memorandum of Understanding with Central Valley Low Income Housing Corp. (CVLIHC) to act as the HMIS Lead Agency and serve as the HMIS Administrator. (See attached CoC/HMIS Lead MOU).

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) prior to being provided access to the HMIS. In addition, participating CHO personnel must receive training by the HMIS Lead Agency and each person granted access to HMIS is required to sign an **End-User Agreement** (Appendix C) prior to being provided access. Independent researchers or research agencies requesting access to SJCoC's HMIS will require approval by the SJCoC Board of Directors.

SJCoC HMIS Lead Agency

The HMIS Lead Agency is responsible for the organization and management of the HMIS, under the terms of an MOU with the SJCoC and is responsible for all system-wide policies, procedures, communication, and coordination. It is also the primary contact with HMIS vendor, and with its help, will implement all necessary system-wide changes and updates.

The HMIS Administrator is the primary position in the management of the SJCoC HMIS. Responsibilities include:

- Providing training support to CHO/Participating Agencies by determining training needs of Users, developing training materials, and training Users in equipment and software;
- Providing technical support to CHO/Participating Agencies;
- Managing user accounts and access control;
- Identifying and developing system enhancements and communicating changes to CHO/Participating Agencies;
- Communicating system-related information to all CHO/Participating Agencies; and
- Developing and modifying reports for Users;
- Ensuring data quality.

CHO/Participating Agency representatives

Each CHO/Participating Agency must designate in writing to the HMIS Administrator the name and contact information of the authorized representative responsible for the oversight of all personnel that generate or have access to client data in the SJCoC HMIS to ensure adherence to the Policies & Procedures described in this document. The authorized representative is responsible for:

- Signing the Agency Partner Agreement and Data Sharing Memorandum of Understanding prior to program implementation and Users being granted access;
- Ensuring organizational adherence to the Policies and Procedures;
- Monitoring compliance with standards of confidentiality and data collection, entry, and retrieval;
- Serving as the primary contact between Users and HMIS Administrator;
- Notifying all members of their organization of any system-wide changes and other relevant information;
- Notifying the HMIS Administrator of personnel changes within three (3) business days;
- Communicating needs and questions regarding the SJCoC HMIS to the HMIS Administrator in a timely manner.
- Detecting and responding to violations of the Policies and Procedures.

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 CHO/Participating Agency 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 CHO/Participating Agency.
- Agencies that are inactive with client entry for more than 30 days may have user and/or agency 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 and made active, live data entry must begin within fifteen days.

- Mandatory reporting entities/subrecipients/Participating Agencies are **solely** responsible for entering required data into the HMIS, for informing the HMIS Lead Agency of their need to be included in the HMIS, and for taking the necessary steps/returning necessary paperwork to be set up in the HMIS to meet the requirements of their contract(s)
- Data entered into the SJCoC HMIS remains the property of the SJCoC even after a CHO/Participating Agency terminates its agreement with the SJCoC. The SJCoC and remaining Participating Agencies shall maintain their right to the use of all client data previously entered by the terminating CHO/Participating Agency, subject to any restrictions requested by the client.

SJCoC HMIS PRIVACY POLICY AND DATA SHARING POLICY

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 I, and should be made available to clients upon request.

Not all SJCoC stakeholders have direct access to HMIS; direct access is provided only to CHOs that are direct providers of services under the structure of these policies and procedures; funding sources that contract/subcontract with other agencies/individuals who are tasked by the contract to provide those direct services are not considered "direct providers." 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 de-identified, 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.

The HMIS Lead Agency will endeavor in good faith to answer requests by Public Agencies by producing reports generated from the HMIS to provide information regarding homelessness within the SJCoC. Resulting reports will utilize only de-identified, aggregate data. The HMIS Lead Agency will, to a reasonable extent, also endeavor in good faith to answer requests by SJCoC stakeholders with reports generated from the HMIS to provide information regarding homelessness within the SJCoC. Resulting reports will utilize only de-identified, aggregate data. The HMIS Lead Agency is not mandated to provide reports to Public Agencies or SJCoC stakeholders, and the HMIS Lead Agency is the sole arbiter regarding the reasonableness of requests from Public Agencies and SJCoC stakeholders and whether to respond to those requests.

Direct sharing of data contained in the HMIS is not allowed, except under the express direction of the SJCoC Board of Directors following the strict process established by the SJCoC under the Data-Sharing Agreement (Appendix H).

Protection of PII is of extreme importance to the SJCoC. This document explains to clients and Participating Agencies the circumstances under which PII may be shared without express consent. The Privacy Posting (Appendix E) describes generally the conditions under which client data may be shared, including PII, and shall be posted publicly by each Participating Agency.

Federal law may require participating agencies to have their own agency-specific privacy policies. Information entered and accessed by the Collaborative Applicant 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. All amendments apply retroactively. 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. The HMIS Lead Agency may share client information on an HMIS-wide basis (or on a subset thereof) if the HMIS Lead Agency determines the sharing of data is to provide enhanced services, including case management, health care, and/or housing, and if the agency/organization receiving the client information has completed the process described in the Data Sharing Agreement (Appendix H) and is determined to have met the requirements therein. The HMIS Lead Agency may share client information on an HMIS-wide basis to meet mandatory reporting requirements of the federal and state governments, including but not limited to Longitudinal Systems Analysis, System-wide Performance, Housing Inventory Count, Point in Time Count, and others as determined by the HMIS Lead Agency.
- **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, endangerment, 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 or do not wish to share their information any longer (, it is their responsibility to let their case manager or intake worker know, who must then take the proper action to honor that request and to document that client's request appropriately.

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.

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 (Internet Service Provider) 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 (Pretty Good Privacy) 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. Users need to contact the HMIS Lead Agency for reinstatement.

- 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 written procedures to handle client paper records and submit them to the HMIS Lead Agency. 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 user, date, and time of access. The HMIS Lead Agency will at least monthly review all user access privileges; users who have not access the system within thirty (30) days of the review will have access suspended.

Local Physical Safeguards

- The HMIS Lead Agency and CHOs will take all reasonable, foreseeable and protective actions to physically secure the PII of clients. These actions are listed below but do not represent an exhaustive list of physical safeguards.
  1. To secure PII when transmitting written communication about clients, all users will use the client unique identifier automatically generated by the HMIS to refer to the client.
  2. Hard copies of client information or reports with PII 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 HMIS Lead Agency 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.

Local Technical Safeguards

- The HMIS Lead Agency and CHOs will take all reasonable, foreseeable and protective actions to technically secure the PII 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 every 90 days.
  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 out of the SJCoC HMIS after 20 minutes of inactivity.
  5. Electronic documents stored outside of a private protected local network that contain PII 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 PII associated with clients for data no longer in use and notify the appropriate CHO.

Local HMIS Security Plan

Prior to being given access to HMIS all users must participate in a basic end user security training. The training will be provided by someone at the HMIS Lead Agency 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 PII 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 HMIS Lead Agency 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 Agency for further resolution. If the user and the CHO's authorized representative is the same person, then that person will contact the HMIS Lead Agency 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 an 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. 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.

DATA QUALITY AND AGENCY PARTICIPATION

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

Identification of Participating Agencies

Mandatory reporting entities/subrecipients are solely responsible for entering required data into the HMIS in a timely and accurate manner, for informing the HMIS Lead Agency of their need to be included in the HMIS, and for taking the necessary steps/returning necessary paperwork to be set up in the HMIS to meet the requirements of their contract(s)

Recipients of funds that mandate Subrecipient participation in the HMIS are responsible for making clear to Subrecipients of any obligation to report via the HMIS. Recipients are solely responsible for directly informing all Subrecipients that they are mandated to record Universal Data Elements for all persons served into the HMIS at the time of an award of funds. Recipients shall inform the HMIS Lead Agency of all Subrecipients and CHOs that are mandated to enter data into the HMIS. Recipients include, but are not limited to, the Collaborative Applicant, San Joaquin County, and the City of Stockton.

The HMIS Lead Agency is responsible for working with identified Subrecipients to ensure Subrecipients are properly set up and trained to enter data into the HMIS, and for providing as-needed ongoing technical support. The HMIS Lead Agency is not responsible for entering data on behalf of any Participating Agency.

Subrecipients that are mandated to enter data into the HMIS are responsible for responding to the HMIS Lead Agency, including but not limited to inquiries regarding data entry, data quality, and the set-up of agency, project, service, and assessment functions within the HMIS.

Agencies that are not mandated reporting entities but desire to participate in the HMIS shall directly contact the HMIS Lead Agency. To be considered for HMIS participation, non-mandated entities must submit a written statement explaining the need for HMIS participation, the benefits to the agency, the benefits to the community/SJCoC, and the number of licenses sought. The HMIS Lead Agency will make a determination regarding HMIS participation. Agencies denied HMIS participation by the HMIS Lead Agency may appeal to the Data and HMIS Committee, which may make a determination of appeal on behalf of the SJCoC.

Timeliness of Data

To be 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

In order to report 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. 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 Data 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

All Recipients of funds that mandate HMIS participation should include these expected Data Completeness Standards in their notices of funding and contracts with Subrecipients. Potential Subrecipients should be directly informed regarding the mandate to collect all Universal Data Elements for all individuals served by a project. Potential Subrecipients should be directly informed of this mandate by Recipients through notices of funding, notices of award, and initial contact by the Recipients informing Subrecipients of their required participation in the HMIS.

Data Accuracy (Data Validity)

Information entered into HMIS needs to be valid, i.e. it needs to accurately represent information on the clients of the homeless service programs contributing data to HMIS. 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.

Data Consistency

Consistency is the degree to which the data is collected and stored in a uniform manner, across all users of the HMIS. If users do not have a shared understanding of when, how, and why data should be collected in an HMIS, then it is likely that the data will not be accurate.

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 CoC HMIS and Data Committee may authorize the HMIS Lead Agency to negotiate unilaterally. The cost of access by mandatory reporting entities may be less than that for voluntary reporting entities.

Fee schedules for participation may be approved by the SJCoC Board of Directors and implemented by the HMIS Lead Agency as directed by the SJCoC Board.

Agency and User Inactivity

Limited resources require strategic use of HMIS user and agency licenses. Therefore, any HMIS user who is not active for 30 days or more may have their status switched to "Inactive" and their license allocated to another user or project; this action may be taken unilaterally by the HMIS Lead Agency without the need to consult the user or agency. Also, any agency that has no active users for 30 days or more may have their status switched to "Inactive" and their license(s) allocated to another/other user(s) or project(s); this action may be taken unilaterally by the HMIS Lead Agency without the need to consult the agency. Reactivation fees may be charged by the HMIS Lead Agency at its discretion.

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.