Sacramento Continuum of Care
HOMELESS MANAGEMENT INFORMATION SYSTEM

STANDARD OPERATING POLICIES AND PROCEDURES

Table of Contents

HMIS Lead Agency Contact Information

Sacramento Steps Forward (SSF)
2150 River Plaza Drive, Suite 385
Sacramento, CA 95833
www.sacramentostepsforward.org

HMIS Contact Information	Team Contact Email Reason
Rolf Davidson, Director of Programs rdavidson@sacstepsforward.org (916)233-1734	1. Operational leadership of SSF's HMIS, grants, and contracts.
HMIS Inbox HMIS@sacstepsforward.org	1. Requests for support related to data quality and management. 2. General technical support for HMIS issues related to user access, troubleshooting, information requests, system functionality errors, etc. 3. Training 4. Requests for issues related to data quality, management and/or mandated reports, report failure, etc. 5. Requests for issues related mandated reports, report failure, etc.

Introduction

This document provides the framework for the ongoing operations of the Sacramento Continuum of Care (CoC) Homeless Management Information System Project (HMIS). The ***Project Summary*** provides the main Objectives, direction and benefits of HMIS System while the ***Governing Principles*** establishes the values that are the basis for all policy statements and subsequent decisions.

Operating procedures provides specific policies and steps necessary to control the operational environment and enforce compliance in:

- Collection and entry of consumer data
- HMIS Pparticipation
- Release and disclosure of consumer data
- Server availability
- Server security
- Workstation security
- Technical support
- Training availability
- User authorization and passwords

Project Summary

A. Background: Congressional Requirements

In accordance with Congressional requirements, the U.S. Department of Housing and Urban Development (HUD) requires the development and maintenance of a local Homeless Management and Information System (HMIS) of all communities receiving Homeless Assistance Grants and organized as a Continuum of Care (CoC).

HMIS is an electronic data collection system designed to store longitudinal consumer-level data about the people accessing homeless services in a CoC. With the ability to integrate and de-duplicate data from all homeless assistance and homelessness prevention programs in a community, it can provide the means to understand the size, characteristics, and needs of Sacramento's homeless population.

The key function of the HMIS is to document the demographics of homelessness in Sacramento according to the HUD Data Standards. With this information, it is possible to identify patterns in service utilization and to document the effectiveness of services and, by extension, to support and improve the delivery of homeless services in Sacramento. The following list highlights other related functions and benefits of the HMIS system:

- **Improvements in service delivery** for consumers as case managers assess the consumer's needs, inform the consumer about available services on site or through referral, help the consumer find and keep permanent housing, and improve service coordination when information is shared between programs within one agency that are serving the same consumer.
- **A confidential and secure environment** that protects the collection and use of all consumer data including personal identifiers.
- The **automatic generation of standard reports** required by HUD, SSF, or other community partners, including Sacramento's contribution to the Annual Homeless Assessment Report (AHAR).
- **Generation of system-level data and** analysis of resources, service delivery needs and program outcomes for the Sacramento's homeless population.
- A **data collection and management tool** for partner agency to administer and supervise their programs.

The Sacramento Continuum of Care (CoC) is the coalition of homeless housing and service providers whose programs constitute the heart of the community's response to homelessness, as well as the community planning body required by HUD in order to receive HUD McKinney Vento funding. Meeting the needs of homeless persons served by the members of Sacramento's CoC is the underlying and most basic reason for maintaining the HMIS, along with employing it for continued improvements in program quality.

On behalf of the Sacramento CoC, Sacramento Steps Forward (SSF) is responsible for staffing and administering the County's Homeless Management and Information System. SSF is the authorizing agency for all agreements made between partner agencies and SSF. SSF's HMIS department – the HMIS System Administrator – are responsible for roll-out and management of the system, including coordination, training, and user access. The HMIS department will also make provisions for technical assistance to users of the system throughout the County.

B. Overview HMIS Software

In Sacramento, HMIS implementation began with a community-wide planning process. At conception, the Sacramento County Department of Human Assistant (DHA) served as the HMIS Administrator. As part of the Sacramento County and Cities Board on Homelessness, DHA convened a planning process to identify the high level requirements for the County's HMIS and to select a software vendor, ultimately contracting with Bitfocus. Sacramento Steps Forward assumed responsibility of HMIS Administration in 2012. At the time of the transfer, the system was compliant with the March 2010 HUD Data Standards and was capable of generating reports and unduplicated counts of services, which provide a statistical profile of homeless services and consumers. The

system continues to be compliant with all HUD Data Standards, including the latest revisions published in December 2021 for the 2022 HUD Data Standards.

The Clarity Human Services Case Management Software uses a web-enabled application residing on a central server to facilitate data collection by homeless service providers in various geographic locations. Access to the central server is limited to those agencies formally participating in HMIS, including only authorized staff members who have met the necessary training and security requirements. In late summer, 2015, the partner agencies of the Sacramento CoC agreed to an "open" HMIS system. Since that time all partner agencies, with the exception of those who fall under HIPPA regulations, have been able to view a client's demographic and programmatic history of all other agencies that participate in the system.

Who is Bitfocus?

Bitfocus is a system integration and development consultancy, providing custom software development, database management, report development, technical assistance, and many other tasks not just exclusive to HMIS.

What is Clarity Human Services Case Management Software

The Clarity is a database management system developed by Silver Spur Systems LLC, a separate firm from Bitfocus that was established when METSYS was purchased. Both Bitfocus and Silver Spur are owned by Robert Herdzig. Clarity operates as a Cloud Service: a software application that is provided as a live service through a web browser such as Internet Explorer, Firefox, Safari or Chrome, rather than a product you need to download and install. This means wherever authorized users are, only the internet and your secure login details are required to access the Clarity database management system.

HMIS Computer Requirements

Partner agencies commit to a reasonable program of data and equipment maintenance in order to sustain an efficient level of system operation. Partner agencies must meet the technical standards for minimum computer equipment configuration:

- Internet connectivity.
- Computers in public areas used to collect and store HMIS data must be staffed at all times.
- Password protected screen savers must be automatically enabled when the workstation is not in use.
- Written information pertaining to user access should not be stored or displayed in any publicly accessible location.
- Data Storage: The partner agency agrees to only download and store data in a secure environment.
- Data Disposal: The partner agency agrees to dispose of documents that contain identifiable consumer level data by shredding paper records, deleting any information from all equipment before disposal, and deleting any copies of consumer level data from the hard drive of any machine before transfer or disposal of property.

Clarity takes advantage of the latest in web technologies. For both security and compatibility, it is extremely urgent that your local IT staff ensure all workstations are outfitted with the latest version of the web browser you use.

Internet Browsers Requirements

The following web browsers are supported by Clarity:

- Microsoft – Edge on Windows 10 106.0.1370.34
- Microsoft – Edge on MacOS 6.0.1370.34
- Mozilla – Firefox 105.0.3

- Google – Chrome 106.0.5249.92
- Apple – Safari 16.0.3

System access over wired networks: Access to the HMIS **system over wired networks** will be controlled using a hardware based firewall. While HUD does not specify specific parameters, Bitfocus will use its best reasonable efforts to use the highest level of security reasonably attainable between the Sacramento CoC system and partner agencies. If an agency is not large enough to warrant a hardware firewall, each client workstation accessing the HMIS system will be required to have a locally installed firewall.

System access over wireless networks: Access to the HMIS system over any type of wireless network is discouraged. Wireless networks are more susceptible to unauthorized access than wired networks. If any type of wireless network is used, it must have at least 128-bit encryption. If 128-bit encryption is not available, each client workstation must have VPN client software installed.

B. Governing Principles

HMIS system relies upon the following governing principles:

- Confidentiality: The rights and privileges of consumers are crucial to the success of HMIS. Following these policies and procedures ensure consumer privacy without impacting the delivery of services. This is the primary focus of agency programs participating in HMIS. Policies regarding consumer data are founded on the premise that a consumer own his/her/their own personal information and provide the necessary safeguards to protect consumer, agency, and policy-level interests. Collection, access, and disclosure of consumer data through HMIS will only be permitted by the procedures set forth in this document.
- Data Integrity: Consumer data is the most valuable and sensitive asset of the HMIS. These policies are designed to ensure data integrity and protect information from accidental or intentional unauthorized modification, destruction, or disclosure.
- System Availability: The availability of a centralized data repository is necessary to achieve the optimal type of aggregation of unduplicated homeless statistics across the county. SSF staff are responsible for ensuring the broadest deployment and availability of the system for homeless service agencies in the Sacramento CoC.
- Compliance: Violation of the policies and procedures set forth in this document will have serious consequences. Any deliberate or unintentional action resulting in a breach of confidentiality or loss of data integrity may result in the withdrawal of system access for the offending entity.

SSF recognizes the need to maintain each consumer's confidentiality and will treat the personal data contained within the HMIS with respect and care. SSF has both an ethical and a legal obligation to ensure that data is collected, accessed and used appropriately. Of primary concern to SSF are issues of security (i.e. encryption of data traveling over the internet, the physical security of the HMIS server), and the policies governing the release of this information to the public, government and funders.

C. General HMIS User and Partner Agencies Responsibilities

Because HUD awards points in the annual Notice of Funding Opportunity (NOFO), a competition based on HMIS performance, incomplete or inaccurate reports can and will affect the awarding of points within the CoC. NOFO is an announcement of funding available for a particular program or activity. Sacramento CoC has been successful in receiving full points with respect to HMIS, and we must continue to expand and improve upon our use of the system to ensure long-term success in the face of increasing requirements. In the future, we will be expected to generate a wider array of statistical reports at the program and community level. As such, data quality and accuracy is of utmost importance and begins at the user level. To maintain data integrity, when applicable, SSF

hosts a HMIS user group to keep providers updated regarding changes to the system, overall data quality, and any issues or problems that require user input to resolve. The group also serves as a forum for users to raise concerns or challenges. SSF provides HMIS trainings on an ad hoc basis, depending on user needs.

All SSF and HUD funded providers are required to participate in the HMIS. Participation is defined as the entry of all HUD-required data elements for all consumers served. The list of required data elements is maintained in the HUD Data Standards which is communicated to the HMIS users by the HMIS department, with the assistance of the partner agencies administrators.

Data must be entered into the HMIS on a timely basis.

- For emergency shelter providers, data should be entered no more than forty-eight (48) hours after the provision of the service or from program exit.
- For transitional housing or permanent housing, data should be entered no more than three (3) days after the provision of the service or from program exit.

Programs serving consumers for over a year must update those fields outlined in the HUD Data Standards (program-level data elements) at a frequency determined by HUD. At the time of writing, CoC programs required annual updates and Homelessness Prevention and Rapid Re-Housing Program (HPRP) programs required quarterly updates, but these requirements are subject to change.

All SSF and HUD-funded homeless housing and service providers are required to produce Annual Performance Reports (APRs) (and other monthly or quarterly reports requested/required by SSF) directly from the HMIS, with the exception of Victim Service Providers (VSPs).

D. Use of a Comparable Database by "Victim Service Providers"

Exceptions to the above are programs that specifically target to service individuals fleeing or attempting to flee a domestic violence situation. These programs can be exempt for using HMIS in accordance with the Department of Justice Reauthorization Act Victims Against Women Act (VAWA) of 2005. Victim Service Providers (VSP) are prohibited from entering Personal Protected Information (PPI) into an HMIS. Instead, the organizations are required to use a relational database that is comparable to the HMIS. To be truly a comparable database, it must be a relational database that meets all the HMIS data standards and the minimum standards of the HMIS privacy and security requirements. It also must be able to produce the comma-separated values (.csv) files required to submit an Annual Performance Report (APR) and Consolidated Annual Performance and Evaluation Report (CAPER).

- Any CoC grant with at least one VAWA provider project sponsor must submit an APR with two sections, one for the VAWA provider(s) and one for the others. If your grant has at least one VAWA provider project sponsor and at least one non-VAWA provider project sponsor, the grantee must effectively submit two APRs. E-SNAPS will prompt the grantee to complete the two reports if the grantee indicates at the outset that one (or more) of the sponsors is a VAWA provider.
- The VAWA provider generates a report using a comparable database for all persons served for each grant. If a grantee has more than one project sponsor that is a VAWA provider, the APR data must be aggregated into one VAWA provider APR or "DV APR." The DV APR is entered into E-SNAPS by the grantee.
- Although a grantee with both non-VAWA and VAWA project sponsors will submit separate VAWA and non-VAWA consumer data, total financial information (for the grantee and all sponsors) is submitted at once.
- HUD requires that the Program Descriptor Data for each homeless assistance program within the CoC operated by a victim service provider must be recorded in the HMIS, with the exception of the street address of a facility that provides victim services to consumers.

If an organization receives any funds from the Office of Violence Against Women (OVW) programs, Office for Victims of Crime (OVC) programs, or Family Violence Prevention and Services Act (FVPSA) despite having a

different mission, the organization still may be prohibited from entering PPI into the HMIS, depending on how the funding is used. If it is used organization-wide or for the organization's administrative purposes, all programs operated by the organization, regardless of program type, are prohibited from entering PPI into the HMIS and would use a comparable database instead.

VAWA states that "Personally identifying information (PPI) includes information such as an individual's name, address, other contact information, and social security number, but it also can include information such as an individual's race, birth date, or number of children if, in the particular circumstances, that information would identify the individual. Personally identifying information also may include information that is encoded,encrypted, hashed, or otherwise protected." Finally, HUD does not have authority over VAWA regulations.

For Technical Assistance related to VAWA, please reach out to the Safe Housing Partnerships. Additional information can be found on the Safe Housing Partnerships website.

1.0 - Roles and Responsibilities

1.1 - HMIS Lead Agency Responsibilities

Policy: The HMIS lead agency will be responsible for the organization and management of the HMIS.

Responsibilities:

- The HMIS lead agency is responsible for all system-wide policies, procedures, communication, and coordination. It is also the primary contact with Bitfocus, and with its help, will implement all necessary system-wide changes and updates.
- In this role as lead agency, SSF oversees the operation of a uniform HMIS that yields the most consistent data for consumer management, agency reporting, and service planning.
- Each HMIS System Administrator will agree to abide by standard operating procedures, confidentiality and ethics of the HMIS.
- All concerns relating to the policies and procedures of the HMIS should be brought to the SSF's HMIS Program Manager. However, the CEO/Executive Director of SSF is the final authority for policies and procedures of the HMIS.

The success and utility of HMIS is dependent upon a number of different actors/roles, as outlined below.

1.1a - HMIS Program Manager

Policy: The HMIS Program Manager is a member of the HMIS Department whose primary responsibility is the overall oversight and administration of the HMIS. The SSF HMIS Program Manager serves as the primary liaison with partner agency, coordinates the HMIS team, and oversees the provision of reports and other data to the staff and members of SSF. The HMIS Program Manager reports to the Director of Programs.

Responsibilities:

- Coordination of HMIS user licenses for partner agencies;
- Management of Memoranda of Understanding (MOU) with partner agencies;
- User administration, including adding and removing partner Agency Administrator;
- Ensuring proper training of all HMIS users (documentation, confidentiality, reporting, etc.);
- Providing technical support such as trouble-shooting;

- Maintenance of a list of Agency Administrator for all partner agencies to ensure the ability to communicate regularly with all participating organizations;
- Oversight of community-level reporting related to HMIS participation, bed coverage, and other required information;
- Oversight of program descriptors in HMIS as set out by the HUD Data Standards. Responsible for maintaining program descriptors and the bed inventory for any agencies listed on the Housing Inventory Count (HIC) that is not an HMIS partner agency;
- Ensure that HMIS matches the CoC-approved Housing Inventory Count (HIC);
- Insure HMIS Policy & Procedures manual is maintained, and updated as community makes additions or changes to HMIS policy;
- Oversee/ensure the development of reports (whether performed internally or outsourced).

1.1b - HMIS Coordinator

Policy: The HMIS Coordinator provides essential technical and analytical support to the HMIS Program Manager, conducting regular review of both community and program-level data. The HMIS Coordinator reports to the HMIS Program Manager.

Responsibilities:

- Creation of project forms, documentation, and other key tools used by partner agencies ensure compliance with US Department of Housing and Urban Development (HUD) regulations governing HMIS;
- Providing training and technical support to users to ensure proper use of HMIS;
- Assisting in the generation and submission of program and community-level reports from HMIS, including HMIS components of all HUD applications, the Point-in-Time Counts, the LSA, etc.;
- Analysis of data for internal reporting and monitoring as needed;
- Conducting regular data quality reviews to monitor overall system data quality;
- Working closely with partner agencies to address data issues, and improve data quality;
- Conducting data quality trainings as needed;
- Other HMIS support functions as needed.

1.1b - HMIS Customer Support

Policy: The HMIS Customer Support Specialist supports the operations of the HMIS by providing day-to-day support to internal and external system users. The HMIS Coordinator reports to the HMIS Program Manager.

Responsibilities:

- Provide technical, analytical, and clerical support on administrative support activities;
- Provides daily support to system users via email, phone, and video conferencing;
- Data quality and database cleansing projects, creating and revision of forms and other tools to ensure compliance with US Department of Housing and Urban Development (HUD) regulations governing HMIS;
- Enhances processes to streamline various types of implementations, i.e., user accounts, training, programs, and internal workflows;

- Conducts regular reviews to monitor overall system utility;
- Provides staff support to HMIS committees and workgroups including meeting announcements, agenda preparation in consultation with the HMIS Program Manager, taking meeting minutes, and preparing other meeting materials.
- Other HMIS support functions as needed.

1.1c - HMIS Lead Agency Communication with Partner Agency

Policy: The HMIS Department is responsible to communicate any system-related information to partner agencies in a timely manner.

Procedure:

- HMIS team will send email communication to the Agency Administrator;
- Agency Administrator are responsible for distributing information and ensuring that all members of their agency are informed of appropriate HMIS related communication;
- Specific communications will be addressed to the person or parties involved;
- Each HMIS lead agency will also distribute HMIS information on their designated website.

1.2 - Software Vendor (Bitfocus)

Policy: The software vendor (Bitfocus) is responsible for the set-up, operation, and maintenance of the HMIS software platform.

Responsibilities:

- Addressing any technical problems that arise with respect to the Bitfocus software and/or functionality;
- Provide system and application updates to ensure the ability of the HMIS to comply with all HUD reporting requirements;
- Interface with the HMIS Program Manager to ensure that HUD required reports are submitted within deadlines, including (but not limited to) AHAR, HPRP QPR and APR, performance reporting for Sacramento's HUD SHP Exhibit I application, and SHP APR and technical submissions;
- Interface with the HMIS Program Manager and ensure access to data quality reports that encompass all data fields necessary to successfully submit the above-mentioned reports;
- Interface with HMIS team to ensure that the system meets the needs of the partner agencies;
- In coordination with the HMIS Program Manager, monitor system access and, as needed, manage user access to maintain security;
- Interface with HMIS Program Manager to coordinate data imports/exports via the HUD XML import standard;
- Strive to maintain continuous availability to HMIS by design, by practice, and utility;
- Provide system security as set out by the HUD technical standards in regards to server, system and user access;
- Schedule necessary and planned downtime when it will have least impact, for the shortest possible amount of time, and will be coordinated with SSF. A minimum of one week notice shall be given to SSF to allow coordination with partner agencies;

- Schedule major upgrades in coordination with SSF. Any upgrade that has a significant impact on HMIS user training or the HMIS user's experience shall require a minimum of 60 day notice to SSF;
- Design and implement a backup and recovery plan (including disaster recovery);
- Oversee recovery from unplanned downtime, communicating, and avoiding future downtime;
- Comply with any new HUD Data or Technical Standard within 30 days of delivery of the final approved standard;
- Consider and implement enhancements or customizations to HMIS at the request of SSF. Respond to SSF within 30 days, notifying them of any additional costs and/or implications of the enhancements/customizations requested;
- The HMIS software vendor's employees will agree to abide by all confidentiality and ethics standards.

1.3 - Partner Agency

Policy: Partner agencies are those agencies that use HMIS for the purposes of data entry, data editing and data reporting. Relationships between the HMIS lead agency and partner agencies are governed by any standing agency-specific agreements or contracts already in place, the HMIS Partner Agency Agreement and the contents of the HMIS Policies and Procedures. All partner agencies are required to abide by the policies and procedures outlined in this manual

Responsibilities:

Prior to obtaining access to the HMIS system, every partner agency must adopt the following:

- Designate a staff member to be the HMIS Agency Administrator who is responsible on a day-to-day basis for enforcing the data and office security requirements under the policies outlined in this manual. Only one person per authorized agency may be designated as the Agency Administrator;
- Comply with **HUD Data and Technical Standards**;
- **HMIS Partner Agency Agreement** – The agreement made between the partner agency Executive and the local CoC governing body which outlines agency responsibilities regarding their participation in the HMIS. This document is legally binding and encompasses all state and federal laws relating to privacy protections and data sharing of consumer specific information;
- **Inter-Agency Data Sharing Agreement** – Must be established between agencies for sharing of consumer level data above and beyond the minimum shared elements (central intake) takes place;
- **HMIS End-User Agreement** – Signed by each HMIS user, the user will agree to abide by standard operating procedures and ethics of the HMIS;
- **Consumer Notice** – Each partner agency will post a written explanation describing the policies regarding mandatory collection of consumer data to be stored on the HMIS;
- **Privacy Notice** – Each partner agency will post a written explanation describing the agency's privacy policies regarding data entered into the Sacramento HMIS System;
- **Consumers Informed Consent & Release of Information Authorization Form** – Must be implemented and monitored by agencies and would require consumers to authorize in writing the entering and/or sharing of their personal information electronically with other participating agencies throughout the Sacramento CoC HMIS where applicable;

- **HMIS Privacy Statement** – A written explanation of privacy practices and security measures that will be enforced to protect the consumer's information on the HMIS. This statement should be handed to the consumer at time of entry into the system;
- **Grievance Form** – The consumer has a right to file with the local CoC governing body if the consumer feels that the partner agency has violated their rights;
- When applicable, **Transfer of Data Agreement** – The agreement made between the partner agency Executive Director and the local CoC governing body to transfer, upload, or migrate data from the agency's existing system to the HMIS;
- All agencies will be subject to periodic on-site security assessments to validate compliance of the agency's information security protocols and technical standards.

1.3a - Partner Agency's Staffing Responsibilities

Each partner agency will need to have staff to fulfill the following roles and all functions must be assigned and communicated to the HMIS System Administrator. Each partner agency is responsible for ensuring they meet the Privacy and Security requirements detailed in the HUD HMIS Data and Technical Standards. Annually, each partner agency will conduct a thorough review of internal policies and procedures regarding HMIS.

1.3b - Partner Agency Security Officer

Policy: Each partner agency must designate a Security Officer to oversee HMIS privacy and security at the agency level.

Responsibilities:

- In conjunction with the partner Agency Administrator, work with the HMIS System Administrator to ensure that each agency HMIS users read, understand and sign the HMIS End-User Agreement and that they are appropriately trained, including proper usage of HMIS and full awareness of and compliance with privacy and security standards.
- Conducts security audits of all workstations and work devices used for HMIS as well conduct the annual system security audit;
- Assumes responsibility for reporting any misuse of the software by agency staff to SSF;
- Assumes responsibility for posting both the **Privacy Notice** and the **Consumer Notice;**
- Assumes the responsibility for the maintenance and disposal of on-site computer equipment.

1.3c - Partner Agency Administrator

Policy: Each partner agency must designate an Agency Administrator who will be responsible for the oversight of all personnel that generate or have access to client data in the HMIS to ensure adherence to the policies and procedures described in this document.

Responsibilities:

- Serve as the primary contact between the partner agency and SSF;
- Maintains an individualized agency email address and be a licensed user;
- Assumes responsibility for posting **Privacy Notice** that describes the mandatory collection requirements;
- Manage agency user licenses and coordinating with the HMIS System Administrator regarding adding and removing licensed users for their agency. Agency Administrator are required to notify an HMIS System

Administrator to remove licensed users from the HMIS immediately upon termination from agency, placement on disciplinary probation, or upon any change in duties not necessitating access to HMIS information;

- Secure access to all consumer data, user data and agency administration information on behalf of the partner agency, thus assuming responsibility for the quality and accuracy of these data;
- In conjunction with the partner agency Security Officer, work with the HMIS System Administrator to ensure that all agency HMIS users read, understand and sign the HMIS End-User Agreement and that they are appropriately trained, including proper usage of HMIS and full awareness of and compliance with privacy and security standards;
- Provide support for the generation of agency reports, including Agency level HUD reporting;
- Monitor and enforce compliance with standards of consumer confidentiality and ethical data collection, entry, and retrieval at the agency level;
- Maintain program descriptor information in HMIS as set out by the HUD Data Standards;
- When applicable, attend monthly HMIS user meetings and workshops;
- Periodically reviews system access control decisions.

1.3d - HMIS End-User

Policy: Each partner agency must designate end-users to enter the data at the agency level.

Responsibilities:

- Completes training on the appropriate use of the HMIS system prior to accessing the system;
- Acknowledges an understanding of this Policies and Procedures Manual;
- Adheres to any agency policies that affect the security and integrity of consumer information;
- Is responsible for agency's HMIS data quality. Data quality refers to the timeliness of entry, accuracy and completeness of information collected and reported in HMIS;
- Signs HMIS End-User Agreement and any other required forms prior to accessing system;
- Reports system problems and data-related inconsistencies to Agency Administrator or HMIS System Administrator as appropriate.
- Obtains consumer signature on the Consumers Informed Consent & Release of Information Authorization;
- When applicable, gives consumer written copy of **HMIS Privacy Statement**;
- Verbally communicates consumer's rights and uses of consumer's data;
- When applicable, attend monthly HMIS user meeting and workshops.

1.3e - Partner Agency Communication with HMIS Lead Agency

Policy: The partner agency is responsible for communicating needs and questions regarding the HMIS to the HMIS System Administrator a timely manner.

Procedure:

- Partner agency will send email communication to HMIS@SacStepsForward.org;
- Specific communications will be addressed to the person or parties involved.

2.0 - Policies and Procedures Implementation

2.1 - HMIS Partner Agency Agreement Requirement

Policy: The Executive Director of a partner agency shall follow, comply, and enforce the HMIS Partner Agency Agreement and this agreement must be signed prior to being granted access to the HMIS.

Procedure:

- An original signed HMIS Partner Agency Agreement must be presented to the HMIS System Administrator before any program is implemented in the HMIS;
- After HMIS Partner Agency Agreement is signed, the HMIS System Administrator will train the agency's designated HMIS users on the use the HMIS;
- A username and password will be granted to HMIS users after required training is completed;
- Signing of the HMIS Partner Agency Agreement is a precursor to training and user access;
- The SSF HMIS Administrator will update the list of all partner agency and make it available to the project community.

2.2 - HMIS User Agreement Requirements

Policy: HMIS users of any partner agency shall follow and comply with the HMIS End-User Agreement. The HMIS user must sign this agreement before being granted access to HMIS. This form is available on the SSF website at www.sacstepsforward.org under the Request New Users tab.

Procedure:

- The HMIS System Administrator will provide the Agency Administrator and/or the agency Security Officer the HMIS Staff Verification for HMIS Access form and the HMIS End-User Agreement. The HMIS Staff Verification for HMIS Access form should be scanned to the HMIS team at HMIS@sacstepsforward.org no later than two (2) days prior to the training date. Both forms must be signed by either the employee's supervisor, the Agency Administrator, the agency Security Officer or the Executive Director.
- Prior to the user being granted access to the system, a HMIS System Administrator will collect and maintain both originals of the HMIS Staff Verification for HMIS Access form and the HMIS End-User Agreement. SSF will maintain copies of both forms for all HMIS users.

The Agreement submits the following:

- The user understands and agrees that they may not publish, disclose, or use any information collected for or contained within the HMIS except as permitted by the SSF HMIS procedures or applicable by law.
- The user understands and agrees that all passwords and/or other security measures assigned to them are to be used solely by them, and are not to be disclosed to or utilized by any other individual.
- The user understands and agrees that if they knowingly and intentionally violate the confidentiality provisions of applicable rules and regulations, they may be subject to termination and/or liability under applicable law.
- The user understands and agrees that their obligations under the agreement shall remain in effect following any termination of the agreement or of their employment with the agency listed on the form.

The user must also receive a copy of the Consumer Notice and the HMIS Privacy Statement and must agree to comply with all provisions contained within them. All agencies will use the Consumer Notice form, available on the SSF website, and post it in a visible spot at all points of intake.

2.3 - Site Security Assessment

- Prior to allowing access to the HMIS, the partner Agency Administrator and SSF staff will review and assess the security measures in place to protect consumer data.
- This meeting may include, but is not limited to: the partner agency Executive Director (or designee), the partner agency Security Officer, the manager, and the Agency Administrator with SSF staff member (or designee) to assess agency information security protocols.
- This review shall in no way reduce the responsibility for agency information security, which is the full and complete responsibility of the partner agency, its Executive Director, and the Agency Administrator.
- Agencies shall have virus protection software on all computers that access HMIS.

2.4 - Data Collection Requirements

Policy:

- Partner agencies will collect and verify the minimum set of data elements for all clients served by their projects.

Procedure:

- Partner agencies of Emergency Shelters must enter data into the system within 48 hours of intake or exit and partner agency of Transitional Housing and Permanent Supported Housing projects must enter data into the system within 72 hours of intake or exit.
- In Central Intake, HMIS users must collect all the universal data elements set forth in the 2022 HUD Data Standards.

The universal data elements include:

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

- HMIS users must also collect all the program-specific data elements at program entry and exit set forth in the 2022 HUD Data Standards.

The program-specific data elements include:

4.2	Income and Sources	4.11	Domestic Violence
4.3	Non-Cash Benefits	4.12	Current Living Situation
4.4	Health Insurance	4.13	Date of Engagement
4.5	Physical Disability	4.14	Bed-Night Date
4.6	Developmental Disability	4.15	Financial Assistance Provided
4.7	Chronic Health Condition	4.19	Coordinated Entry Assessment

4.8 HIV/AIDS
4.9 Mental Health Disorder
4.10 Substance Abuse Disorder
4.20 Coordinated Entry Event

2.5 - Technical Support Protocol

Support requests include problem reporting, requests for enhancements (features), or other general technical support. SSF will only provide support for issues specific to the HMIS software and systems.

Policy: Each HMIS lead agency will provide technical support to all partner agency as needed. The process for requesting technical support or making technical recommendations is as follows:

Procedure:

1. HMIS users should first seek technical support from the Agency Administrator.
2. If more expertise is required to further troubleshoot the issue, Agency Administrator will contact the HMIS System Administrator.
3. Technical support hours are Monday through Friday (excluding holidays) from 9:00 am to 5:00 pm.
4. The Agency Administrator will provide issue details if possible (or help recreate the problem by providing all information, screenshots, reports, etc.) in order for the HMIS System Administrator to recreate the problem.
5. The HMIS System Administrator will try to respond to all email inquiries and issues within 3 business days, but support load, holidays, and other events may affect response time.
6. The HMIS System Administrator will submit a ticket to vendor if progress is stalled.
7. If the support request is deemed by the HMIS Administrator to be an agency-specific customization, (agency-specific customizations include but are not limited to new assessments, new data fields, and new pick-lists), resolution of the request may be prioritized accordingly. SSF reserves the right to charge on an hourly basis for these changes if/when the workload for such agency-specific customizations becomes burdensome.
8. SSF staff may at this point determine that the cause of the reported issue is outside the scope of control of the HMIS software and systems.
9. SSF staff will consolidate such requests from multiple partner agency, if appropriate, and strive to resolve issues in priority order according to their severity and impact.
10. If the SSF staff is unable to resolve the issue, other software or system vendor(s) may be included in order to resolve the issue(s).
11. In cases where issue resolution may be achieved by the HMIS user or other partner agency personnel, SSF staff will provide instructions via email to Agency Administrator.

3.0 - Security Policies and Procedures

3.1 - Partner Agency's Responsibilities

- HMIS users participating in the HMIS shall commit to abide by the governing principles of the HMIS and adhere to the terms and conditions of the HMIS Partner Agency Agreement.
- The Agency Administrator must only request user access to HMIS for those staff members that require access to perform their job duties.
- All users must have their own unique user ID and should never use or allow use of a user ID that is not assigned to them.

- User specified passwords should never be shared and should never be communicated in any format.
- New user IDs must require password change on first use.
- The use of default passwords on initial entry into the HMIS application is allowed so long as the application requires that the default password be changed on first use. Written information specifically pertaining to user access (e.g., username and password) shall not be stored or displayed in any publicly accessible location.
- For HMIS users, requests for passwords to be reset will be made via telephone or by e-mail, generated by the user's email address on file to the HMIS System Administrator.
- Three (3) consecutive unsuccessful attempts to login will disable the user ID until the account is reactivated by waiting 60 minutes or by the HMIS System Administrator.

3.2 - Who is HMIS User?

HMIS user is anyone who is provided access to the HMIS system. User access will be granted only to those individuals whose job functions require legitimate access to the HMIS. Each HMIS user will sign an HMIS End-User Agreement and satisfy all the conditions herein before being granted access to the HMIS

3.2a - User Activation

HMIS users require a unique username and password. The HMIS System Administrator will set up a unique username/ID along with temporary password for each partner agency user upon completion of training and receipt of the signed HMIS Staff Verification for HMIS Access form and HMIS End-User Agreement. The sharing of user name and password will be considered a breach of the HMIS End-User Agreement.

3.2b - Request New User ID/Username

Partner agencies may add new users of the HMIS System to the list of authorized users by completing HMIS New User Registeration form.

- The partner agency will determine which of their employees need access to the HMIS.
- Identified users must sign the HMIS End-User Agreement stating that he/she has received training, will abide by the HMIS Policies and Procedures, will appropriately maintain the confidentiality of consumer data, and will only collect, enter and retrieve data in the HMIS relevant to the delivery of services to people in housing crisis in the area served by the partner agency.
- The HMIS System Administrator will be responsible for the collection and storage of signed HMIS End-User Agreement. An electric signature copy will be retained to the user's HMIS account.

3.3 - Password Requirements

The HMIS System Administrator will issue a temporary password for each partner agency user. The user will be prompted to create a new password upon first login. Passwords must be no less than eight (8) characters in length, and must meet the following criteria:

- Minimum 8 characters in total length
- Contain upper-case letters (i.e., H)
- Contain lower-case letters (i.e., h)
- Contain Numbers (ie., 9)
- Cannot contain your first or last name
- Contain special characters (e.g. ~ ! @ # $ % ^ & * ( ) _)

- Not using, or including, the username, the HMIS name, or the HMIS vendor's name
- Not consisting entirely of any word found in the common dictionary or any of the above spelled backwards

3.3a - Forced Password Change (FPC)

The FPC will occur upon first log on with temporary password and FPC will occur every ninety (90) consecutive days. Passwords will expire and user will be prompted to enter a new password. Users may not use the same password consecutively, but may use the same password more than once.

3.3b - Reset Password

- If an user forgets their password, they can use the "Forgot Password" option on the HMIS Login Page.
- If an user has reason to believe that someone else has gained access to their password, they must immediately notify HMIS System Administrator.
- The HMIS System Administrator will reset the user's password and notify the user of their new temporary password.

3.4 - Unsuccessful logon

- If an user unsuccessfully attempts to logon three (3) times, the user ID will be “locked out”, access permission revoked, and user will be unable to gain access for 60 minutes or until their password is reset by the HMIS System Administrator.

3.5 - Change User Access

- When the Agency Administrator determines that it is necessary to change a user's access level they will update the user ID as needed.

3.6 - Rescind User Access

- In the event than an HMIS user breaches the End-User Agreement, violates policies and procedures, breaches confidentiality or security, leaves the agency, or becomes inactive otherwise, the HMIS System Administrator will de-activate the user ID.

4.0 - Operational Policies and Procedures

4.1 - User Access Levels

Policy:

Each HMIS user will be designated an user access level that controls the level and type of access the user has within the HMIS.

Procedure:

- HMIS System Administrator, in consultation with the partner agency, will assign the level and type of access the user will have in the system.
- Agency Administrator is required to communicate to HMIS System Administrator when HMIS user’s need for access changes.
- HMIS System Administrator will terminate access upon receiving notification from the Agency Administrator.
- HMIS System Administrator will revoke user access to anyone suspected or found to be in violation of the policies outlined in this document or the HMIS End-User Agreement.

- The table below lists the levels of access categories tied to existing user roles across the partner agency. Consult with HMIS System Administrator to learn which user access levels are available, as well as other customizable roles that may be offered in consultation and with approval from the HMIS System Administrator.

User Role Categories	Level of Access	Description
System Administrator(s)	Access to all libraries and pages within the HMIS.	This role will grant access to system-wide data in order to support all partner agency, meet reporting requests, and other system administration responsibilities.
Agency Administrator	Access to Central Intake, Agency Services, and other system libraries.	This role will grant access to data collected by their own agency.
Agency Staff Mangement	Access to Central Intake and Agency Services libraries.	This role will grant access to data collected by their own agency.
Client Data Entry	Access only to Central Intake Library and Agency Services libraries.	This role will grant access to data collected by their own agency.
Report & Monitoring	Access only to Management and/or Ad-hoc Reports.	This role will only allow generating reports. Cannot enter and/or modify client data.
Read/View	Access to Central Intake, Agency Services, and other system libraries.	The role will grant access to view data only.

4.2 - Training/HMIS User Group Meetings

Policy:

Each HMIS user must complete the required training and any additional training relevant to their position prior to gaining access to the HMIS. HMIS System Administrator will provide training or coordinate training prior to all HMIS users from partner agency using the HMIS.

Procedure:

- HMIS System Administrator will provide a standard user training to prospective HMIS users. This course focuses on policies and procedures, review of HUD Data and Technical Standards, privacy and mandatory collection notices and consents. The training will include how to navigate HMIS and management of reports.
- HMIS users must successfully complete the standard user training and pass an quiz that demonstrates proficiency in the system and understanding of the policies and procedures.
- HMIS System Administrator will provide new HMIS user with a copy of the Policies and Procedures and HMIS user guide.
- When applicable, ongoing trainings will be provide to HMIS users and Agency Administrator as needed.

4.3 - HMIS End User Group

When applicable, the HMIS user group meets on a monthly basis to assist HMIS users with technical issues, convey news and updates that relate to HMIS usage, review data quality, share best practices, conduct technical trainings as needed, and address any other important issues that pertain to the persons entering data into the HMIS.

4.4 - Assign Agency HMIS Administrator

- The partner agency shall designate, in writing, an Agency Administrator for communications regarding HMIS and submit this documentation to the SSF.
- SSF HMIS Administrator will obtain all signatures necessary to execute the HMIS Partner Agency Agreement.
- SSF will maintain a file of all submitted documentation.
- The HMIS department will maintain a list of all assigned Agency HMIS Administrator and make it available to the SSF project staff.

4.4a - Re-Assign Agency HMIS Administrator

- The partner agency may designate a new or replacement Agency Administrator in the same manner as above.

4.5 - Terminating Participation

4.5a - Voluntary Termination

- The partner agency shall inform the HMIS Administrator in writing of their intent to terminate their agreement to participate in HMIS.
- The HMIS Administrator will revoke access of the partner agency staff to the HMIS.

  Note: All partner agency-specific information contained in the HMIS system will remain in the HMIS system.
- The SSF Executive Director will keep all termination records on file with the associated Memorandums of Understanding (MOUs).

4.5b - Lack of Compliance

- When the HMIS Administrator determines that a partner agency is in violation of the terms of the partnership, the Executive Director of the partner agency and SSF will strive to resolve the compliance issue(s) within 30 days of the conflict(s).
  - Any deliberate or unintentional action resulting in a breach of confidentiality or loss of data integrity may result in immediate withdrawal of system access for the offending entity. In this case, HMIS System Administrator will immediately inform the partner agency, and instigate the peer review process within 48-hours to work with the partner agency to resolve the issue. This action should only be considered in extreme cases.
- If the Executive Directors are unable to resolve the compliance issue(s) within 30 days, the peer review process will be employed to resolve the conflict. If that results in a ruling of termination:
  - The partner agency will be notified in writing of the intention to terminate their participation in the HMIS.
  - The HMIS Administrator will revoke access of the partner agency staff to the HMIS.
  - The SSF Executive Director will keep all termination records on file with the corresponding memorandums of understanding.

4.6 - Confidentiality and Security Plan

4.6a - Security

The data, information, consumer records and related documents stored electronically in connection with the HMIS is confidential and shall be handled as follows:

- All partner agency shall comply with all Federal, State, and Local laws and regulations pertaining to the confidentiality of information and records to ensure that consumer records are protected and not subject to disclosure except as permitted by such laws and regulations. The agencies shall only release consumer records to non-partner agencies with written consent by the consumer, unless otherwise provided for in the relevant laws and regulations.
- All agencies shall comply with all Federal, State, and Local confidentiality laws and regulations as they pertain to:
  - All medical conditions, including but not limited to: mental illness; alcohol and/or drug abuse; HIV/AIDS testing, diagnosis, and treatment; and other such covered conditions; and
  - A person's status as a victim of domestic violence.
- All agencies agree not to release any individual consumer information obtained from the HMIS to any organization or individual without prior written consent of the consumer, unless otherwise required or permitted by applicable law or regulation. Such written consumer consent shall be documented using the HMIS Consumers Informed Consent & Release of Information Authorization. Information that is not approved for disclosure in writing by the consumer shall not be released.
- Only authorized users may view or update data.
- Each adult member of a household that is receiving housing or services will be expected to sign the HMIS Consumers Informed Consent and Release of Information Authorization prior to initial data entry or updating.
- Consent for data entry/updating for minors will be provided for in the parent/guardian's consent form.
- The consent form must be renewed annually for consumers still receiving housing and/or services.
- A consumer may revoke the consent form at any time.
- A consumer always has the right to view his or her own data and to request corrections.
- All agencies shall ensure that all staff, volunteers, and other persons who are issued a user ID and password for the HMIS receive annual confidentiality training regarding consumer information and records.
- If any partner agency, Agency Administrator, HMIS System Administrator, or Bitfocus System Administrator determines that any staff, volunteer, or other person with a user ID has willfully committed a breach of HMIS system security or consumer confidentiality, the HMIS Administrator shall immediately revoke his or her access to the HMIS database. The HMIS Administrator may then review the Agency's policies, procedures, and records to ensure that individuals found have willfully committed a breach of system security or consumer confidentiality are prohibited from accessing the system.
- All Agencies agree that all computer workstations that access the HMIS will be password protected and that the operating system will be locked when users are not at their workstations. Additional measures shall be taken to ensure that data is not visible to other persons while users are accessing the HMIS.
- All HMIS data must be securely stored when not in use, regardless of the media on which the information is recorded.

4.6b - Privacy

The rights and privileges of consumers are of utmost importance to HMIS and crucial to its success. Policies regarding consumer data are founded on the premise that a consumer owns their own Personally Identifying Information and shall provide the necessary safeguards to protect interests on the consumer level as well as agency and policy levels.

4.6b(i) - What is Personally Identifying Information (PPI)

There are five pieces of information that are known as "personal identifying information:" a person's name, social security number, zip code, date of birth, and gender. HMIS uses these pieces of information to uniquely identify consumers within the system. Consumers are not required to grant permission to share personal identifying information for use in HMIS. However, consumers may be required to provide personal identifying information to prove eligibility for a program or service. Consumers will receive services from a partner agency whether or not they agree to share personal identifying information for use in HMIS.

4.6c - Consumers Rights

Consumers have the right to see and receive a copy of the information that the HMIS maintains about them, except for information compiled in anticipation of litigation, information about another individual, information obtained under a promise of confidentiality, or information that would, if disclosed, endanger the life or safety of another. SSF will consider changing any information about a consumer if they believe that the recorded information is inaccurate.

Consumers served by agencies participating in the HMIS have the following rights:

4.6c(i) - Communication

- Consumers have a right to privacy and confidentiality
- Consumers have a right to not answer any questions unless entry into the Agency's program requires it.
- Consumer information may not be shared without informed consent (posting of **Privacy Notice** and a signature authorizing that the client is willing to share their information between partner agency on the HMIS Consumers Informed Consent & Release of Information Authorization).
- Every consumer has a right to an understandable explanation of the HMIS and what "consent to participate" means. The explanation shall include:
  - Type of information collected
  - How the information will be used
  - Under what circumstances the information will be used
  - That refusal to provide consent to collect information shall not be grounds for refusing entry to the program.
  - A copy of the consent shall be given to the consumer upon request and a signed copy kept on file at the partner agency, if applicable.
  - A copy of the **Privacy Notice** shall be made available upon consumer request.
  - A copy of the Statement of Consumer Rights shall be made available upon consumer request.

4.6c(ii) - Participation Opt Out

- Consumers have a right not to have their personal identifying information in the HMIS shared outside the agency, and services cannot be refused if the consumer chooses to opt out of participation in the HMIS. However, consumers may be refused program entry for not meeting other agency eligibility criteria.
- In the event that a consumer previously gave consent to share information in the HMIS and chooses at a later date to revoke consent (either to enter or to share), a HMIS Consumers Informed Consent & Release of Information Authorization must be completed and kept on file.

4.6c(iii) - Disclosure of Information/Access to Records

No consumer shall have access to another consumer's records within the HMIS. However, parental/guardian access will be decided based upon existing agency guidelines An agency may not share any information about the consumer entered by other agencies.

HUD regulations and the Sacramento Continuum of Care's privacy policy provide for a consumer to receive a copy of all information in the HMIS about the consumer. Parents and/or guardians may request a disclosure of information for a minor. This procedure describes the process for a consumer to obtain the information.

- The consumer may make a request for information at the partner agency's office. The agency must then supply a copy of the request form to the consumer and, if necessary, help them complete the request. The request must specify the name and social security number (if known), and HMIS Consumer ID of the person for whom the disclosure is requested. When requesting information for another person, the requestor must state the relationship (i.e. parent, guardian, conservator, etc.). The request form must be signed and dated.
- The completed form can be mailed or faxed to the HMIS Administrator, who has 2 weeks from receipt of the request to respond. The HMIS System Administrator will print all the requested information and place it into a sealed envelope to be picked up by the requestor. The requestor must positively identify themselves to the HMIS Sysyem Administrator or designee before they can receive the printed material. The request and acknowledgement must be maintained in the HMIS Administrator's files for a term of not less than 5 years from the date of receipt by the HMIS Administrator.

4.6c(iv) - Consumer Grievances

Policy:

The consumer has the right to file a grievance with an agency. Consumer will file HMIS-related grievances with the partner agency. The partner agency must have written grievance procedures that can be provided to client upon request. Any unresolved grievances may be escalated to the local HMIS lead agency.

Procedure:

- Clients will submit grievance directly to the partner agency with which they have a grievance.
- Upon client request, the partner agency will provide a copy of their grievance procedure and the HMIS Policies and Procedures.
- The partner agency will be responsible to answer any questions and complaints regarding the HMIS. A record of all grievance and any attempts made to resolve the issue must be kept in file.
- If the grievance is resolved, the partner agency will include the date and a brief description of the resolution. For any written complaint, the partner agency must send a copy to the local HMIS lead agency.
- If the partner agency is unable to resolve the problem, the client must complete the Grievance Form

outlining the date of incident, name of parties involved, description of the incident, and their contact information for follow- up. partner agency must forward a copy of the completed Grievance Form to the local HMIS lead agency.

- The HMIS lead agency will review and determine the need for further action.

5.0 - Data Policies and Procedures

5.1 - Data Collection and Entry of Consumer Data

- Consumer data will be gathered according to the policies, procedures, and confidentiality rules of each individual program.
- Consumer data may only be entered into the HMIS with the consumer's authorization to do so.
- Consumer data will only be shared with partner agency if the consumer consents by signing the Consumer Consent/Release of Information form, and that form is filed on record.
- Consumer identification should be completed during the intake process or as soon as possible following intake and entered into the system within 48 – 72 hours (48 hours for emergency shelter, 72 hours for other participating programs).
- All consumer data entered into the HMIS will be kept as accurate and as current as possible.
- Hardcopy and electronic files will continue to be maintained according to individual program requirements in accordance with the HUD Data Standards.
- No data may be imported without the consumer's authorization.
- Any authorized data imports will be the responsibility of the partner agency.
- Partner agencies for the accuracy, integrity, and security of all data input by said Agency.
- Anonymous Client Data Entry: In the event that a client does not want to have any of their information entered into HMIS, they will be entered under and assumed first and last name, the date of birth shall be 01/01/XXXX, where the XXXX is the actual year of birth and their SSN shall be 999-99-9999. All of the information entered into the system fields will be “client refused”. The HMIS will assign them a unique personal identifier.
- Sharing of Information: Clients must consent to the sharing of their information prior to allowing that information to be shared with partner agency. In the event that the client agrees to have their information entered into the HMIS but does not agree to have it shared with other agencies, the partner agency must select the “Make Case Private” option when enrolling them into their project.

5.2 - Release and Disclosure of Consumer Data

- Consumer-specific data from the HMIS system may be shared with partner agencies only when the sharing agency has secured a valid HMIS Consumers Informed Consent & Release of Information Authorization from that consumer authorizing such sharing. Other non-HMIS inter-agency agreements do not cover the sharing of HMIS data.
- Sharing of consumer data may be limited by each CoC confidentiality rules.
- No consumer-specific data will be released or shared outside of the partner agencies unless the consumer gives specific written permission or unless withholding that information would be illegal. Note that services may not be denied based on the consumer's refusal to sign the form or state any information.
- Consumer shall be given print out of all HMIS data relating to them upon written request and within 10 working

days from the time the written request is received. Written requests will be date/time stamped immediately upon receipt.

- Consumer identifying information will be removed upon written request within 10 working days from the time the written request is received. Written requests will be date/time stamped upon receipt.
- A log of all external releases or disclosures must be maintained for seven years and made available to the consumer upon written request within 10 working days from the time the written request is received. Written requests will be date/time stamped immediately upon receipt.
- Aggregate data that does not contain any consumer specific identifying data may be shared with internal and external agents without specific permission. This policy should be made clear to consumers as part of the informed consent procedure.
- Each agency Executive Director is responsible for their agency's internal compliance with the HUD Data Standards
- Printed Information: Printed records disclosed to the client or another party should indicate: the person and/or agency to whom the record is directed, the date, and the initials of the person making the disclosure.

5.3 - Workstation Security Procedures

- Most security breaches are due to human error rather than systematic issues. In order to keep the application and data secure, HMIS users must also implement some additional security measures. The Agency Administrator is responsible for taking the necessary actions for preventing the degradation of the system resulting from viruses, intrusion, or other factors under the agency's control.
- Agency Administrator is responsible for preventing inadvertent release of confidential consumer-specific information. Such release may come from physical, electronic or even visual access to the workstation, thus steps should be taken to prevent these modes of inappropriate access. HMIS user's computer screens should be placed in a manner where it is difficult for others in the room to see the contents of the screen. (i.e. don't let someone read over your shoulder; lock your screen).
- Definition and communication of all procedures to all agency users for achieving proper agency workstation configuration and for protecting their access by all agency users to the wider system are the responsibility of the Agency Administrator.
- At a minimum, any workstation accessing the HMIS shall have anti-virus software with current virus definitions and frequent full-system scans (weekly).
- Do not write down your username and password and store it in an insecure manner.
- Do not post your HMIS user name or password information under your keyboard, on your monitor, or laying out for others to see. This type of behavior can lead to large security breaches.
- Don't ever share your login information with anybody (including Site or Project Managers).
- If someone is having trouble accessing HMIS, direct them to send an e-mail to the HMIS@SacStepsForward.org.
- Sharing usernames and passwords, or logging onto a system for someone else is a serious security violation of the HMIS End-User Agreement.
- HMIS users are responsible for all actions taken in the system utilizing their logons. With the auditing and logging mechanisms within HMIS any changes anyone makes or actions that are taken will be tracked back to your login.

- When you are away from your computer log out of HMIS or lock down your workstation. Stepping away from your computer while you are logged into HMIS can also lead to a serious security breach. Although there are timeouts in place to catch inactivity built into the software, it does not take effect immediately. Therefore, anytime when you leave the room and are no longer in control of the computer, you must log out of HMIS.

5.4 - HMIS DATA QUALITY STANDARDS

Policy:

All data entered into the Sacramento CoC HMIS must meet data quality standards as set forth in the HMIS Data Quality Plan. Users will be responsible for the quality of their data entry.

Definition:

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

Data Timeliness:

HMIS users must enter all universal data elements and program-specific data elements within 48 hours of intake for Emergency Shelters and 72 hours for Transitional and Permanent Housing Projects.

Data Completeness:

All data entered into the system is complete.

Data Accuracy:

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

Procedure:

- Partner agencies must sign the HMIS Partner Agency Agreement to ensure that all participating programs are aware and have agreed to the data quality standards.
- Upon agreement, partner agencies will collect and enter as much relevant client data as possible for the purposes of providing services to that client.
- The HMIS System Administrator will conduct random checks for data quality. Any patterns of error or missing data will be reported to the Agency Administrator.
- HMIS users will be required to correct the identified data error and will be monitor for compliance by the Agency Administrator and the HMIS System Administrator.
- HMIS users may be required to attend additional training as needed.

The Data Quality Standards provide a framework for ensuring that our community implements procedures that result in good quality HMIS data. These standards apply to the HMIS lead agency, CoC membership and partner agency. The data quality Standard is intended to achieve the following HUD reporting policies:

5.4a - Monitoring by HMIS Lead Agency

The HMIS lead agency will monitor the overall data quality of the HMIS and the quality of the data produced by partner agency. Specifically the lead agency will:

- Utilize various reports to monitor data quality for each program.
- Produce quarterly program level information for each participating program identifying data quality weaknesses and recommending solutions for issues that need to be addressed.
- Provide regular feedback to partner agency to ensure problems are addressed.

- Provide training and/or technical assistance to partner agency to ensure problems are addressed.
- Monitor the cleaning and updating of consumer data that has been identified as non- compliant with the consumer local data quality standards.

5.4b - Reduce Duplications in HMIS

The burden of *not* creating duplicate records falls on each partner agency. In order to reduce the duplication of client records, HMIS users should always search for the client in HMIS before creating a new client record. If matches are found, the user must determine if any of the records found, match their client. Having multiple (duplicate) records on the database for a single client causes confusion and inaccurate information being stored.

- When an HMIS user is entering data from a client, the HMIS user will first attempt to locate that client on the system by searching for client **using partial name, date of birth, last four digits of the social security number or any combination.**

  Best Practices: Start off with 1st two letters of first and last name. "Less is More" meaning less information you enter to search a client will be better to eliminate differing interpretations of birth date, social security number.
- If no matches are found on the database for this client, the HMIS user will continue to add the basic Universal Data elements for the client's intake.

5.5 - Data Use

Data contained in the HMIS will only be used to support the delivery of services to at risk and homeless consumers in the Sacramento County area. Each HMIS user will affirm the principles of ethical data use and consumer confidentiality as noted below and contained in the HMIS End-User Agreement.

5.5a - Data Use by Vendor

- The vendor and its authorized subcontractor(s) shall not use or disseminate data contained within the HMIS without express written permission
- To enforce information security protocols and to ensure that HMIS data is used only with explicit permission and if permission is granted, will only be used in the context of interpreting data for research and for system troubleshooting purposes, the Service and License Agreement signed by the software vendor contains language that prohibits access to HMIS data except under the conditions noted above.

5.5b - Data Use by Agency

- As the guardians entrusted with consumer personal data, HMIS users have a moral and a legal obligation to ensure that the data they collect is being gathered, accessed and used appropriately.
- It is also the responsibility of each user to ensure that consumer data is only used to the ends to which it was collected: ends that have been made explicit to consumers and are consistent with the mission of the agency and the partner agency to assist families and individuals to resolve their housing crisis.
- Proper user training, adherence to the HMIS Policies and Procedures Manual, and a clear understanding of consumer confidentiality are vital to achieving these goals. All HMIS users will sign an HMIS End-User Agreement before being given access to the system. Any individual or partner agency misusing or attempting to misuse the HMIS data can be denied. Sanctions exist if users violate any laws related to consumer confidentiality.

5.5c - Data Use by CoC

The information consumers consent to give to CoC providers for use in HMIS will be used in the following ways:

- By the Continuum of Care, to administer the HMIS, to ensure the data in the system is accurate and valid, to fix problems in the computer system, and to test the system;
- By the Continuum of Care, to prepare reports containing “de-identified” information for the purpose of sharing data and preparing reports for HMIS users, government agencies and policy-makers, and the general public. “De-identified” means that a consumer’s name, social security number, date of birth, address, and any other information that might be used to identify the consumer will not appear in any of the data or reports released by the HMIS user.
- By CoC providers, to verify the accuracy of information entered into the HMIS; and
- By other agencies participating in the HMIS, in order to assist those agencies to more effectively provide and coordinate services.

  In addition to the uses above, CoC providers may also use and disclose information that consumers provide in the following ways:

  - For functions related to payment or reimbursement for services;
  - To carry out internal administrative functions;
  - To create “de-identified” statistical reports;
  - To report abuse, neglect, or domestic violence, but only to the extent that such reports are required by law;
  - To prevent or lessen a serious and imminent threat to the health or safety of person or the public, including the target of a threat, if permitted by applicable law; or
  - To an individual or institution for academic research purposes;

5.6 - Monitoring System Access

The HMIS Administrator will monitor access to system software and regularly review user access privileges and remove identification codes and passwords from the system when users no longer require access.

5.6a - Departing Employees

- When an employee with access to the HMIS ends their employment with a partner agency, the Agency Administrator must notify HMIS SystemAdministrator within 24 hours of their departure to inactivate their access to the HMIS.
- If an employee is to be terminated and the employee has access to the HMIS, the Agency Administrator must notify HMIS Administrator within 24 hours of their departure to inactivate their access to the HMIS.

5.6b - Compliance w/Policy & Procedure

Compliance with these Policies & Procedures is mandatory for participation in the HMIS.

- Using the Bitfocus software, all changes to consumer data are recorded and will be periodically and randomly audited for compliance by SSF staff and Bitfocus.
- When proposed changes originate within a partner agency, they must be reviewed by the partner agency Executive Director, and then submitted by the partner agency Executive Director to the HMIS System Administrator for review and discussion.

5.6c - Request for Policy Addition, Deletion, or Change

All requests for changes to the Policy & Procedure Manual will be made in writing and tracked by the HMIS lead agency staff. Request will be received and reviewed by the lead agency prior to being inserted into the Policy and Procedure Manual.

- All requests for changes, additions, or deletions to the HMIS Policy and Procedure must be submitted in writing in order to be considered. All Sacramento CoC members and partner agency are welcome to submit requests. Submitting a request does not guarantee approval of the request. It is recommended that members who wish to submit a request at which the request will be presented to the user before the final decision.
  - Email HMIS@SacStepsForward.org to request for policy addition, deletion, or change form and submit it to the HMIS System Administrator.
  - Approved requests will be inserted in the HMIS Policy and Procedure Manual and uploaded to the Sacramento Steps Forward website.

HMIS DEFINITIONS

Annual Homeless Assessment Report (AHAR): HUD's annual report to Congress on the nature and extent of homelessness nationwide.

Annual Performance Report (APR): A reporting tool that HUD uses to track program progress and accomplishments of HUD homeless assistance and HPRP Programs on an annual basis (Formerly known as the Annual Progress Report).

Consumer: A living individual about whom a Sacramento COC/partner agency collects or maintains protected personal information: (1) because the individual is receiving, has received, may receive, or has inquired about services from Sacramento COC/partner agency: or (2) in order to identify service needs, or to plan or develop appropriate services within the CoC.

Continuum of Care (CoC): The primary decision making entity defined in the funding applications to HUD as the official body representing a community plan to organize and deliver housing and services to meet the specific needs of people who are homeless as they move to stable housing and maximum self-sufficiency.

CoC Program: A program identified by the CoC as part of its services system, whose primary purpose is to meet the specific needs of people who are experiencing a housing crisis.

Homeless Assistance Program: A program whose primary purpose is to meet the specific needs of people who are literally homeless. Homeless assistance program include outreach, emergency shelter grant, transitional housing, rapid re-housing, permanent housing and permanent supportive housing.

Homeless Prevention Program: A program whose primary purpose is to meet specific needs of people who are at risk of homeless. Homelessness preventions programs include those funded by HPRP and other homelessness prevention programs identified by the CoC as part of its service system.

HMIS User (or users): An employee, volunteer, affiliate, associate, and any other individual acting on behalf of a Sacramento COC, HMIS lead agency, or partner agency who uses or enters data into the HMIS or another administrative database from which data are periodically uploaded to the HMIS.

Homeless Management Information System (HMIS): The information system designated by a CoC to process Protected Personal Information (PPI) and other data in order to create an unduplicated accounting of homelessness within the CoC. An HMIS may provide other functions beyond unduplicated accounting.

HMIS Lead Agency: An organization designated by a CoC to operate the CoC's HMIS on its behalf.

HMIS Participating Bed: For any residential homeless program, a bed is considered a "participating HMIS bed" if the program makes a reasonable effort to record all universal data elements on all consumers served in that bed and discloses that information through agreed upon means to the HMIS lead agency at least once annually.

HMIS Software Solution Provider: An organization that sells, licenses, donates, builds or otherwise supplies the HMIS user interface, application functionality and database.

HMIS Vendor: A contractor who is paid to provide services for the operation of a CoC's HMIS. An HMIS vendor includes an HMIS software solution provider, web server host, and data warehouse provider, as well as a provider of other contracted information technology or support.

Non-Contributory CoC Program: A CoC Program that does not contribute PPI or other consumer-level data to an HMIS.

Participating CoC Program: A contributory CoC Program that makes reasonable efforts to record all the universal data elements and all other required data elements as determined by HUD funding requirements on all consumers served and discloses these data elements through agreed upon means to the HMIS lead agency at least once annually.

Protected Personal Information (PPI): Information about a consumer: (1) whose identity is apparent from the information or can reasonably be ascertained from the information; or (2) whose identity can, taking into account any methods reasonable likely to be used, be learned by linking the information with other available information or by otherwise manipulating the information.

Processing: An operation or set of operations performed on PPI, whether or not by automated means, including but not limited to collection, maintenance, use, disclosure, transmission and destruction of the PPI.

Quarterly Performance Report (QPR): A reporting tool that HUD uses to track progress and accomplishments of HPRP funded programs on a quarterly basis.

Research: A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to general knowledge.

Unduplicated Accounting of Homelessness: An unduplicated accounting of homelessness includes measuring the extent and nature of homelessness (including an unduplicated count of homeless persons), utilization of homelessness programs over time, and the effectiveness of homelessness programs.

Unduplicated Count of Homeless Persons: An enumeration of homeless persons where each persons is counted only once during a defined period of time.

Victim Services Provider: A nonprofit or nongovernmental organization including rape crisis centers, battered women's shelters, domestic violence transitional housing programs, and other programs whose primary mission is to provide services to victims of domestic violence, dating violence, sexual assault, or stalking.

Appendices of Forms

- Appendix A: Agreement between Sacramento Steps Forward and Bitfocus
- Appendix B: HMIS Privacy Statement
- Appendix C: HMIS End-User Agreement
- Appendix D: HMIS Consumers Informed Consent & Release of Information Authorization
- Appendix E: HMIS Consumers Notice (Must be posted at place of intakes, lobbies, or waiting area)
- Appendix F: Revocation of Consent to Release
- Appendix G: Interagency HMIS Data Sharing Agreement (Sacramento CoC Only)
- Appendix H: HMIS Participating Agency List
- Appendix I: HUD HMIS Data Standards

Document History

Date of Revision	Revision Notes
04/2018	Release of the document
01/2023	Review and updates