SACRAMENTO
STEPS FORWARD
Ending Homelessness. Starting Fresh.

HOMELESS MANAGEMENT INFORMATION SYSTEM (HMIS)
HMIS & DATA COMMITTEE MEETING AGENDA
Thursday, July 12th, 2018
10:00 AM – 11:30 AM
1331 Garden Highway, Sacramento, CA 95833
VCR Conference Room (2nd Floor)

| Agenda Item | Notes |
|---|---|
| I. Welcome & Introductions (Dion Dwyer, Chairman) | |
| II. Approval of Minutes (Dion Dwyer, Chairman) | |
| III. Staffing Update<br>a. HMIS Administrator – (Chris)<br>b. Data Analyst (Chris) | |
| IV. Privacy and Security Plan<br>a. Review of changes discussed at last meeting.<br>b. Approval of Plan<br>c. Approval of supporting documents | |
| V. Data Quality Plan<br>a. Review of changes discussed at last meeting.<br>b. Approval of Plan | |
| VI. Data Quality Reporting<br>a. Creation of new dashboards<br>b. Discussion on Timeliness of Data Standards | |
| VII. Review of Yearly HMIS recertification Quiz Draft | |
| VIII. Review of Yearly Security Audit Checklist | |
| IX. HUD Reports<br>a. Point In Time (PIT) and Housing Inventory Chart (HIC) – Submitted<br>b. System Performance Report - Submitted | |
| X. Adjourn<br>a. Next Quarterly HMIS & Data Committee Meeting October 11th, 2018 | |

SACRAMENTO
STEPS FORWARD
Ending Homelessness. Starting Fresh.

# HOMELESS MANAGEMENT INFORMATION SYSTEM (HMIS)
# HMIS & DATA COMMITTEE MEETING AGENDA

Thursday, April 12, 2018
10:00 AM – 11:30 AM
1331 Garden Highway, Sacramento, CA 95833
VCR Conference Room (2nd Floor)

Members Present:

SSF Staff: Michele Watts – Chief of Programs, Christopher Weare – Manager of Data Analytics and Research, Lindsay Moss – Senior HMIS and Data Analyst

Call to Order Dion Dwyer, 10:10

I. Welcome and Introductions: Dion Dwyer and Christopher Weare

II. Data Department Updates

- Chris Weare reports on Matt Foy's departure as HMIS Administrator and start of job search
- Chris Weare and Lindsay Moss demonstrated progress in the construction of dashboards

III. HUD Reports

- HUD reports for the 2018 PIT and HIC Counts are near completion

IV. Privacy and Security Plan

- SSF will send all agencies copies of the privacy statement that they must post to the their sites. Dion pointed out that agencies should send the links to the HMIS Administrator for tracking purposes. SSF will examine whether non-CoC programs are also required to post the privacy statement.
- There was broad support for the SSF recommendation that after 7 years of inactivity client profiles should be retained in the HMIS but made anonymous.
- There were numerous issues raised about requiring renewal of consent for ROI every two years. Committee members support the implementation of the Clarity ROI processes, but there are issues with requiring renewed ROIs every two years. Many clients leave service for multiple years and if their profiles were made private, programs would not have access to their history when they returned for services. Also, others voiced concerns about the administrative burden. The Committee directed SSF staff conduct some further study. They are to check on best practices in the area and assess the number of clients that return after two years. SSF staff will also implement the Clarity ROI process to assess how much that system will reduce the administrative burden of acquiring ROI consent forms. The Committee will revisit this recommendation once additional information is collected. Staff will also investigate whether agencies are mandated to preserve paper ROI forms if those forms are uploaded into the HMIS.
- The committee agreed with the implementation of recommended amendment #2 and #3. SSF will put together an annual audit checklist and circulate it to participating agencies.
- The committee agreed with the 4th amendment that eliminates the requirement for annual training sessions. In its place SSF will implement a yearly quiz implemented with an online survey tool. SSF staff will draft a quiz for the Committee's approval. Individuals who do not pass the quiz (the pass/no pass point was not determined) will be required to view a refresher video.
- The Committee agree with the 5th amendment, the plan to disable user account after 30 days of inactivity. User who login in after that time will require a password reset. SSF staff is committed to performing these resets in a timely manner.

- In the 6th amendment, The Committee agrees with SSF the staff recommendation to create standard encryption protocols.  The Committee suggested that the staff investigate creating a secure FTP site.
- The Committee agree to the 7th proposed amendment that individuals currently experiencing homelessness and receiving services be allowed to become HMIS users if they are hired as service providers.  The Committee did emphasize that the duties of HMIS users should be particularly emphasized with such users, and it recommended that such users receive additional training on the restriction of the use of HMIS data.

Data Quality Plan

- The Committee supported created and publishing data quality scorecards.  Dion suggested that agency names should be masked when reporting these scores publically.

Additional Business

- SHRA requested that at the next meeting, the Committee should review and discuss the data quality standards concerning the timeliness of data.

Next Meeting:  July 12th, 2018  10am – Noon  1331 Garden Highway

SACRAMENTO
STEPS FORWARD
Ending Homelessness. Starting Fresh.

**MEMORANDUM**

**Date:** 7/5/18
**To:** HMIS and Data Committee
**From:** Chris Weare
**Subject:** **Approval of Privacy and Security Plan & Data Quality Plan**

This memo summarizes the changes to the Privacy and Security Plan & Data Quality Plan submitted to the Committee for approval. In addition, the memo outlines changes to procedures and related document that will support the changes to these plans.

**Privacy and Security Plan**

1. The Privacy Statement and the Privacy and Security Plan have been updated to clarify the rules concerning the sharing of PPI with law enforcement officials. The Privacy Statement will be distributed to agencies to post on their websites.
2. The requirement for annual formal HMIS training is replaced with a requirement to complete a quiz on HMIS procedures. Users who fail to score 70% or higher on the quiz or choose not to participate in the quiz will be required to attend an HMIS training session. A draft quiz is attached for review.
3. To abide by a HUD mandate all HMIs records that have been inactive for 7 years will have their PPI removed.
4. The current plan requires clients to renew their consent for the release of information (ROI) every 5 years. While technical advisors at Community Solutions recommended that renewing consents every 2 years was common practice, the Committee requested a review of ROI consent terms by other CoCs. This review found that 7 of 11 agencies had terms of 7 years or more (three had a 3 year term, and one had a 1 year term). We recommend moving the time for which consent remains valid to 7 years which will streamline administration and keep records available for clients who return to homelessness after an extended absence. In the short-run, this change will have little effect on HMIS procedures because all existing consent forms have the 5 year term and only consent forms signed in the future would have the longer term.
5. Agencies are no longer required to designate a security officer. Agencies will be required to conduct an annual audit which includes completing a compliance certification checklist. A draft checklist is included here. Additional agency audits may be conducted by the Lead Security Officer on an as needed basis.
6. HMIS Users will be required to change their password every 30 days or become inactive. We will reserve the right to terminate end user licenses after 30 days of inactivity. We will not do so regularly, but will employ the right to manage the number of users for which SSF is being billed.
7. SSF is in the process of securing a HIPPA compliant cloud file storage solution. Agencies will be encouraged to leave all documents containing PPI on that file storage site.
8. The new plan changes the existing prohibition of individuals who are actively receiving homelessness services from any HMIS partner agency from gaining access to the HMIS. They will be allowed access, but the plan recommends that they receive additional training on the permissible uses of HMIS data.

**Data Quality Plan**

The Data Quality Plan only includes minor changes. It broadens the checks that will be performed to include data quality issues identified by the HMIS administrator, and it proposes posting quarterly reports that include de-identified metrics of program performance. These dashboards will need to be programmed but should be complete by the next meeting of the HMIS Committee.

Attachments: Compliance audit checklist
Annual HMIS Re-certification test
HMIS Privacy Statement (7.5.18) DRAFT
HMIS Privacy and Security Plan Revised 4.3.18
Sacramento Data Quality Plan Draft Revision 6-29-18

# HMIS PRIVACY
# &
# SECURITY PLAN

**Sacramento County CoC**

## PRIVACY & SECURITY

Privacy refers to the protection of the client's data stored in an HMIS from open view, sharing, or inappropriate use. Security refers to the protection of the client's data stored in the HMIS from unauthorized access, use, or modification.

# HMIS Privacy and Security Plan

*Adopted by the Sacramento County Continuum of Care (XXXXX)*

## Contents

## Introduction

The HMIS Lead Agency is responsible for overseeing HMIS privacy and security. The HMIS Lead Agency may delegate some specific duties related to maintaining HMIS privacy and security to an HMIS System Administrator. The HMIS System Administrator is responsible for preventing degradation of the HMIS resulting from viruses, intrusion, or other factors within the System Administrator's control and for preventing inadvertent release of confidential client-specific information through physical, electronic or visual access to Administrator workstations or system servers. HMIS Partner Agencies are responsible for preventing degradation of the HMIS resulting from viruses, intrusion, or other factors within the agency's control and for preventing inadvertent release of confidential client- specific information through physical, electronic or visual access to End User workstations. Each Partner Agency is responsible for ensuring it meets the Privacy and Security requirements detailed in the HUD HMIS Data and Technical Standards. Partner Agencies will conduct a thorough review of internal policies and procedures regarding HMIS semiannually.

# Privacy

## Privacy Plan Overview

On July 30, 2004, the US Department of Housing and Urban Development (HUD) released the standards for Homeless Management Information Systems (69 Federal Register 45888) and on December 9, 2011 HUD released ***HMIS Requirements Proposed Rule*** (***Federal Register / Vol. 76, No. 237 / Friday, December 9, 2011 / Proposed Rules).***

These standards outlined the responsibilities of the HMIS and for the agencies which participate in an HMIS. This section describes the Privacy Plan of the Sacramento County HMIS System. We intend our policy and plan to be consistent with the HUD standards. All users, agencies and system administrators must adhere to this Privacy Plan.

We intend our Privacy Plan to support our mission of providing an effective and usable case management tool. We recognize that clients served by individual agencies are not exclusively that "agency's client" but instead are truly a client of the Sacramento County Continuum of Care. Thus, we have adopted a Privacy Plan which supports an open system of client-level data sharing amongst agencies.

The core tenant of our Privacy Plan is the Baseline Privacy Statement. The Baseline Privacy Statement describes how client information may be used and disclosed and how clients can get access to their information. Each agency must either adopt the Baseline Privacy Statement or develop a Privacy Statement which meets and exceeds all minimum requirements set forth in the Baseline Privacy Statement (this is described in the Agency Responsibilities section of this Privacy Plan). This ensures that all agencies who participate in the HMIS are governed by the same minimum standards of client privacy protection.

| | |
|---|---|
| **Baseline Privacy Statement:** This is the main document of this Privacy Plan. This document outlines the minimum standard by which an agency collects, utilizes and discloses information. | *REQUIRED* Agencies must adopt a privacy statement which meets all minimum standards. It is strongly recommended to post this Statement on your Agency's local website (if available). |
| **Consumer Notice Posting:** This posting explains the reason for asking for personal information and notifies the client of the Privacy Notice. | *REQUIRED* Agencies must adopt and utilize a Consumer Notice Posting. |
| **Consumers Informed Consent & Release of Information Authorization**: This form must be signed by all adult clients and unaccompanied youth. This gives the client the opportunity to refuse the sharing of their information to other agencies within the system. | *REQUIRED* Client Signatures are required prior to inputting their information in HMIS. |

### HMIS User Responsibilities

A client's privacy is upheld only to the extent that the users and direct service providers protect and maintain their privacy. The role and responsibilities of the user cannot be over-emphasized. A user is defined as a person that has direct interaction with a client or their data. (This could potentially be any person at the agency: staff member, volunteer, contractor, etc.)

Users have the responsibility to:

- Understand their agency's Privacy Statement
- Be able to explain their agency's Privacy Statement to clients
- Follow their agency's Privacy Statement
- Know where to refer the client if they cannot answer the client's questions
- Must complete **Consumers Informed Consent & Release of Information Authorization** with client prior collecting HMIS data.
- Present their agency's Privacy Statement client before collecting any information
- Uphold the client's privacy in the HMIS

## Agency Responsibilities

The 2004 HUD HMIS Standards emphasize that it is the agency's responsibility for upholding client privacy. All agencies must take this task seriously and take time to understand the legal, ethical and regulatory responsibilities. This Privacy Plan and the Baseline Privacy Statement provide guidance on the minimum standards by which agencies must operate if they wish to participate in the HMIS.

Meeting the minimum standards in this Privacy Plan and the Baseline Privacy Statement are required for participation in the HMIS. Any agency may exceed the minimum standards described and are encouraged to do so. Agencies must have an adopted Privacy Statement which meets the minimum standards before data entry into the HMIS can occur.

Agencies have the responsibility to:

- Review their program requirements to determine what industry privacy standards must be met that exceed the minimum standards outlined in this Privacy Plan and Baseline Privacy Statement (examples: Substance Abuse Providers covered by 24 CFR Part 2, HIPPA Covered Agencies, Legal Service Providers).
- Review the 2004 HUD HMIS Privacy Standards (69 Federal Register 45888)
- Adopt and uphold a Privacy Statement which meets or exceeds all minimum standards in the Baseline Privacy Statement as well as all industry privacy standards. The adoption process is to be directed by the individual agency. Modifications to the Baseline Privacy Statement must be approved by the HMIS Committee.
- Ensure that all clients are aware of the adopted Privacy Statement and have access to it. If the agency has a website, the agency must publish the Privacy Statement on their website.
- Make reasonable accommodations for persons with disabilities, language barriers or education barriers.
- Ensure that anyone working with clients covered by the Privacy Statement can meet the User Responsibilities.
- ~~Designate at least one Security Officer that has been trained to technologically uphold the agency's adopted Privacy Statement.~~

Each HMIS Partner Agency must have a Privacy Statement that describes how and when the Partner Agency may use and disclose clients' Protected Personal Information (PPI). PPI includes name, Social Security Number (SSN), date of birth, zip code, project entry and/or exit date, and unique personal identification number (HMIS Unique Identifier).

Partner Agencies may be required to collect some PPI by law, or by organizations that give the agency money to operate their projects. PPI is also collected by Partner Agencies to monitor project operations, to better understand the needs of people experiencing homelessness, and to improve services for people experiencing homelessness. Partner Agencies are permitted to collect PPI only with a client's written consent.

Partner Agencies may use and disclose client PPI to:

- Verify eligibility for services,
- Provide clients with and/or refer clients to services that meet their needs,
- Manage and evaluate the performance of programs,
- Report about program operations and outcomes to funders and/or apply for additional funding to support agency programs,
- Collaborate with other local agencies to improve service coordination, reduce gaps in services, and develop community-wide strategic plans to address basic human needs,
- Participate in research projects to better understand the needs of people served.

Partner Agencies may also be required to disclose PPI for the following reasons:

- When the law requires it,
- When necessary to prevent or respond to a serious and imminent threat to health or safety,
- When a judge, law enforcement or administrative agency orders it,

Partner Agencies are obligated to limit disclosures of PPI to the minimum necessary to accomplish the purpose of the disclosure. Uses and disclosures of PPI not described above may only be made with a client's written consent. Clients have the right to revoke consent at any time by submitting a request in writing.

HMIS uses may respond to an oral request from a law enforcement officer for PPI for the purpose of identifying or locating a suspect, fugitive, material witness or missing person. Nonetheless, the only PPI that may only may be shared is the name, address, date of birth, place of birth, Social Security Number, and distinguishing physical characteristics of the individual. No programmatic information including program enrollments, services provided, recent field contacts, or the like may be shared;

Clients also have the right to request in writing:

- A copy of all PPI collected,
- An amendment to any PPI used to make decisions about your care and services (this request may be denied at the discretion of the agency, but the client's request should be noted in the project records),
- An account of all disclosures of client PPI,
- Restrictions on the type of information disclosed to outside partners,
- A current copy of the Partner Agency's privacy statement.

Partner Agencies may reserve the right to refuse a client's request for inspection or copying of PPI in the following circumstances:

- Information compiled in reasonable anticipation of litigation or comparable proceedings,
- The record includes information about another individual (other than a health care or homeless provider),
- The information was obtained under a promise of confidentiality (other than a promise from a health care or homeless provider) and a disclosure would reveal the source of the information,
- The Partner Agency believes that disclosure of the information would be reasonably likely to endanger the life or physical safety of any individual.

If a client's request is denied, the client should receive a written explanation of the reason of the denial. The client has the right to appeal the denial by following the established Partner Agency grievance procedure. Regardless of the outcome of the appeal, the client shall have the right to add to his/her program records a concise statement of disagreement. The Partner Agency shall disclose the statement of disagreement whenever it discloses the disputed PPI.

All individuals with access to PPI are required to ~~complete formal training in privacy requirements at least annually.~~ complete a quiz on HMIS procedures annually. Users who fail to score 70% or above on the quiz will be required to attend an HMIS training

Partner Agency Privacy Statements may be amended at any time. Amendments may affect information obtained by the agency before the date of the change. An amendment to the Privacy Statement regarding use or disclosure will be effective with respect to information processed before the amendment, unless otherwise stated. A record of all amendments to this Privacy Statement must be made available to clients upon request.

This document should, at a minimum, reflect the baseline requirements listed in the HMIS Data and Technical Standards Final Notice, published by HUD in July 2004 and revised in March 2010. In any instance where this Privacy Statement is not consistent with the HUD Standards, the HUD Standards take precedence. Should any inconsistencies be identified, please immediately notify the Sacramento County HMIS Lead Agency, using the contact information below.

All questions and requests related to this Privacy Statement should be directed to: ~~Manjit Kaur~~ Tina Wilton with Sacramento Steps Forward: twilton@sacstepsforward.org or 916.993-7707.

### HMIS Lead Agency: System Administration Responsibilities

HMIS Lead Agency has the responsibility to:

- Adopt and uphold a Privacy Plan which meets or exceeds all minimum standards in the Baseline Privacy Statement.
- Train and monitor all users ~~and Security Officer~~ upholding system privacy.
- Monitor agencies to ensure adherence to their adopted Privacy Plan.
- Develop action and compliance plans for agencies that do not have adequate Privacy Statements.
- Maintain the HMIS Website to keep all references within the Baseline Privacy Statement up to date.
- Provide training to agencies and users on this Privacy Plan.
- Remove all personally identifiable information from user accounts after they have been inactive for 7 years. This PII may be stored in a secure location to enable the system administrator re-identify records if the need arises.

## System Security

### Security Plan Overview

HMIS security standards are established to ensure the confidentiality, integrity and availability of all HMIS information. The security standards are designed to protect against any reasonably anticipated threats or hazards to security and must be enforced by system administrators, agency administrators as well as end users. This section is written to comply with section 4.3 of the 2004 Homeless Management Information Systems (HMIS) Data and Technical Standards Final Notice (69 Federal Register 45888) as well as local legislation pertaining to maintaining an individual's personal information. At this time, in December ~~2013~~2011, HUD has released proposed regulations pertaining to HMIS Security. These regulations are not yet in force and sufficient guidance has not been given to enact the policies.

Meeting the minimum standards in this Security Plan is required for participation in the HMIS. Any agency may exceed the minimum standards described in this plan and are encouraged to do so. All Agency Administrators are responsible for understanding this policy and effectively communicating the Security Plan to individuals responsible for security at their agency.

## Security Plan Applicability

The HMIS System and all agencies must apply the security standards addressed in this Security Plan to all the systems where personal protected information is stored or accessed. Additionally, all security standards must be applied to all networked devises. This includes, but is not limited to, networks, desktops, laptops, mobile devises, mainframes and servers.

All agencies, including the HMIS Lead, will be monitored by the HMIS System Administrators annually to ensure compliance with the Security Plan. Agencies that do not adhere to the security plan will be given a reasonable amount of time to address any concerns. Egregious violations of the security plan may result in immediate termination of an agency or user's access to the HMIS as determined by the HMIS Lead.

## Security Officer~~s~~

The HMIS Lead Agency will designate a Lead Security Officer ~~and all HMIS Partner Agencies must designate Security Officers~~ to oversee HMIS privacy and security. A single point-of-contact who is responsible for annually certifying that Agencies adhere to the Security Plan; testing the CoC's security practices for compliance.

### *Lead Security Officer*

- May be an HMIS System Administrator or another employee, volunteer or contractor designated by the HMIS Lead Agency who has completed HMIS ~~Privacy and Security~~ training that covers Privacy and Security issues and is adequately skilled to assess HMIS security compliance,
- Assesses security measures in place prior to establishing access to HMIS for a new Agency,
- Reviews and maintains file of Partner Agency annual compliance certification checklists,
- Conducts ~~annual~~ security audit of all Partner Agencies, on an as needed basis.

### *Partner Agency ~~Security Officer~~*

***~~May be the Partner Agency HMIS Agency Administrator or another Partner Agency employee, volunteer or contractor who has completed HMIS Privacy and Security training and is adequately skilled to assess HMIS security compliance,~~***

- Conducts a security audit for any workstation that will be used for HMIS purposes,
  - No less than ~~semi~~annually for all agency HMIS workstations, AND
  - Prior to issuing a User ID to a new HMIS End User, AND

- Any time an existing user moves to a new workstation.

- Continually ensures each workstation within the Partner Agency used for HMIS data collection or entry is adequately protected by a firewall and antivirus software (per Technical Safeguards – Workstation Security),
- Completes the ~~semi~~annual Compliance Certification Checklist, and forwards the Checklist to the Lead Security Officer.

Upon request, the HMIS Lead Agency may be available to provide Security support to Partner Agencies who do not have the staff capacity or resources to fulfill these duties. ~~assigned to the Partner Agency Security Officer.~~

## Physical Safeguards

In order to protect client privacy it is important that the following physical safeguards be put in place. For the purpose of this section, authorized persons will be considered only those individuals who have completed HMIS ~~Privacy and Security~~ training within the past 12 months.

- Computer Location – A computer used as an HMIS workstation must be in a secure location where only authorized persons have access. The workstation must not be accessible to clients, the public or other unauthorized Partner Agency staff members or volunteers. A password protected automatic screen saver will be enabled on any computer used for HMIS data entry.
- Printer location – Documents printed from HMIS must be sent to a printer in a secure location where only authorized persons have access.
- PC Access (visual) — Non-authorized persons should not be able to see an HMIS workstation screen. Monitors should be turned away from the public or other unauthorized Partner Agency staff members or volunteers and utilize visibility filters to protect client privacy.
- Mobile Device – A mobile device used to access and enter information into the HMIS system must use a password or other user authentication on the lock screen to prevent an unauthorized user from accessing it and it should be set to automatically lock after a set period of device inactivity. A remote wipe and/or remote disable option should also be downloaded onto the device.

## Technical Safeguards

### *Workstation Security*

- To promote the security of HMIS and the confidentiality of the data contained therein, access to HMIS will be available only through approved workstations.
- The HMIS Lead Agency will enlist the use of an IP Address Whitelist or another suitably secure method to identify approved workstations, in compliance with Public Access baseline requirement in the HUD Data Standards (4.3.1 System Security). End-Users will be required to submit the IP Address of their workstation to the HMIS Lead Agency to be registered into the system and will notify the Lead Agency should this number need to be changed.
- Partner Agency Security Officer will confirm that any workstation accessing HMIS shall have antivirus software with current virus definitions (updated at minimum every 24 hours) and frequent full system scans (at minimum weekly).
- Partner Agency Security Officer will confirm that any workstation accessing HMIS has and uses a hardware or software firewall; either on the workstation itself if it accesses the internet through a modem or on the central server if the workstation(s) accesses the internet through

the server.

***Establishing HMIS User IDs and Access Levels***

- The HMIS System Administrator, in conjunction with the Partner Agency Security Officer, will ensure that any prospective End User reads, understands and signs the HMIS End User Agreement annually. The HMIS System Administrator will maintain a file of all signed HMIS End User Agreements.
- The Partner Agency HMIS Security Officer is responsible for ensuring that all agency End Users have completed a mandatory training~~s~~, that covers~~including~~ HMIS Privacy, Security and Ethics ~~training and~~, End User Responsibilities, and Workflow ~~training~~issues, prior to being provided with a User ID to access HMIS. End-Users must review and sign an HMIS End User Agreement within the HMIS System ~~Administrator~~ on an annual basis.
- All End Users will be issued a unique User ID and password. Sharing of User IDs and passwords by or among more than one End User is expressly prohibited. Each End User must be specifically identified as the sole holder of a User ID and password. User IDs and passwords may not be transferred from one user to another.
- The HMIS System Administrator will always attempt to assign the most restrictive access that allows an End User to efficiently and effectively perform his/her duties.
- The HMIS System Administrator will create the new User ID and notify the User ID owner of the temporary password verbally in person.
- When the Partner Agency determines that it is necessary to change a user's access level, the HMIS System Administrator will update the user's access level as needed.

***User Authentication***

- User IDs are individual and passwords are confidential. No individual should ever use or allow use of a User ID that is not assigned to that individual, and user- specified passwords should never be shared or communicated in any format.
- Temporary passwords must be changed on first use. User-specified passwords must be a minimum of 6 characters long and must contain a combination of upper case and lower case letters, a number and a symbol.
- End users will be prompted by the software to change their password every ~~90~~ 30 days.
- End Users must immediately notify the HMIS System Administrator if they have reason to believe that someone else has gained access to their password.
- Three consecutive unsuccessful attempts to login will disable the User ID until the password is reset. For Agency End Users, passwords should be reset by the HMIS System Administrator.
- Users must log out from the HMIS application and either lock or log off their respective workstation if they leave. If the user logged into HMIS and the period of inactivity in HMIS exceeds 45minutes, the user will be logged off the HMIS system automatically.

***Rescinding User Access***

- The Partner Agency will notify the HMIS System Administrator within 24-hours if an End User no longer requires access to perform his or her assigned duties due to a change of job duties or termination of employment.
- The HMIS System Administrator reserves the right to terminate End User licenses that are inactive for ~~60~~ 30 days or more. The HMIS System Administrator will attempt to contact the Partner Agency for the End User in question prior to termination of the user's license.
- In the event of suspected or demonstrated noncompliance by an End User with the HMIS End

User Agreement or any other HMIS plans, forms, standards or governance documents, the Partner Agency Security Officer shall notify the HMIS System Administrator to deactivate the User ID for the End User in question until an internal agency investigation has been completed. The HMIS Lead Agency should be notified of any substantiated incidents that may have resulted in a breach of HMIS system security and/or client confidentiality, whether or not a breach is definitively known to have occurred.

- Any agency personnel who are found to have misappropriated client data (identity theft, releasing personal client data to any unauthorized party), shall have HMIS privileges revoked.
- The Continuum of Care is empowered to permanently revoke a Partner Agency's access to HMIS for substantiated noncompliance with the provisions of these Security Standards, the Sacramento County HMIS Policies and Procedures, or the HMIS Privacy Statement that resulted in a release of PPI.

### Disposing Electronic, Hardcopies, Etc.

- Computer: All technology equipment (including computers, printers, copiers and fax machines) used to access HMIS and which will no longer be used to access HMIS will have their hard drives reformatted multiple times. If the device is now non-functional, it must have the hard drive pulled, destroyed and disposed of in a secure fashion.
- Hardcopies: For paper records, shredding, burning, pulping, or pulverizing the records so that PPI is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed.
- Mobile Devices: Use software tools that will thoroughly delete/wipe all information on the device and return it to the original factory state before discarding or reusing the device.

### Other Technical Safeguards

- The Lead Security Officer shall develop and implement procedures for managing new, retired, and compromised HMIS account credentials.
- The Partner Agency Security Officer shall develop and implement procedures for managing new, retired, and compromised local system account credentials.
- The Partner Agency Security Officer shall develop and implement procedures that will prevent unauthorized users from connecting to private agency networks.
- Unencrypted PPI may not be stored or transmitted in any fashion—including sending file attachments by email or downloading reports including PPI to a flash drive, to the End User's desktop or to an agency shared drive. All downloaded files containing PPI must be deleted from the workstation temporary files and the "Recycling Bin" emptied before the End User leaves the workstation.
- SSF will make a HIPPA compliant cloud file storage solution available.  Agencies should leave all documents containing PPI on that file storage site.

### Disaster Recovery Plan

Disaster recovery for the Sacramento County Continuum of Care HMIS will be conducted by the HMIS System Administrator with support from the HMIS software vendor as needed. The HMIS System Administrator must be familiar with the disaster recovery plan set in place by the HMIS software vendor.

- The HMIS System Administrator should maintain ready access to the following information:
    - Contact information – Phone number and email address of the software vendor contact person responsible for recovering the Continuum of Care's data after a disaster.
    - HMIS System Administrator responsibilities – A thorough understanding of the HMIS

System Administrator’s role in facilitating recovery from a disaster.

- All HMIS System Administrators should be aware of and trained to complete any tasks or procedures for which they are responsible in the event of a disaster.
- The HMIS System Administrator must have a plan for restoring local computing capabilities and internet connectivity for the HMIS System Administrator’s facilities.
  This plan should include the following provisions.
  - Account information – Account numbers and contact information for internet service provider, support contracts, and equipment warranties.
  - Minimum equipment needs – A list of the computer and network equipment required to restore minimal access to the HMIS service, and to continue providing services to HMIS Partner Agencies.
  - Network and system configuration information – Documentation of the configuration settings required to restore local user accounts and internet access.

## Workforce Security

### HMIS Access to Active Clients

Sacramento has a shared HMIS system providing HMIS Users with access to client’s current or past history from other agencies. Agencies have sought to hire individuals with lived experience of homelessness or who are currently experiencing homelessness. These individuals may be provided access to the HMIS. Nonetheless, because of the broad access to clients’ current or past history to which these individuals will have access, they should be provided additional training on the restrictions on the use of HMIS data.

~~Sacramento has a shared HMIS system and most HMIS Users have access to client’s current or past history from other agencies. With the goal of protecting the security and integrity of the HMIS system and safeguarding the personal information contained therein, beginning January 1st, 2016 SSF will no longer give HMIS access to Individuals who are actively receiving services from any HMIS partner agency with an active record in either the Sacramento or Yolo County HMIS.~~

- ~~HMIS Lead Agency will search the individual in HMIS before issuing a HMIS access.~~
- ~~Individuals who are active in HMIS will be denied HMIS access.~~

## Background Check

### HMIS User Background Check Requirements

The Sacramento CoC recognizes the sensitivity of the data in the HMIS, and therefore requires that the individuals responsible for managing the HMIS be subject to a criminal background check. No prospective end user will be given a HMIS access if he or she has entered a plea of nolo contendere (no contest) or has been found guilty of any fraud (including identity theft) or stalking related felony crimes punishable by imprisonment of one year or more in any state. The background check must include local and state records; agencies are strongly encouraged to include federal records as well. A background check may be conducted only once for each person unless otherwise required and the results of the background check must be retained in the employee’s personnel file.

### Partner Agency Procedure

Agencies must have a policy regarding conducting background checks and hiring individuals with criminal justice histories consistent with HMIS Privacy and Security Plan. HMIS Participating Agencies should not risk the privacy and confidentiality of client information by allowing any individual convicted of fraud or a stalking related crime in any state. In the broadest sense, a fraud is an intentional deception made for personal gain or to damage another individual.

- Background checks that come back with a criminal history should be carefully considered prior to giving an employee access to client information.
- All End Users should have had a background check prior to access being requested to the HMIS by a Partner Agency.
- Criminal background checks must be completed on all new End Users, and the "Background Check Review and Verification Statement" on the New User Request Form must be signed by the HR Department. The New User Request Form must be submitted to the local Lead Agency System Administrator prior to End Users gaining access to the HMIS.

**HMIS Lead Procedure**

The HMIS Lead Security Officer and all Administrators must also undergo criminal background verification. The HMIS Lead will hire individuals with criminal justice histories only to the extent the hire is consistent with any relevant hiring policies of SSF, unless the background check reveals a history of crimes related to identity theft or fraud.

**List of crimes considered to fall in this category**

A staff member's background check revealing a history of following crimes related to identity theft or fraud should not be given access to the HMIS. The Partner Agency's HR Department must only sign the Background Check Review and Verification Statement if staff's background check doesn't reveal a history of following crimes related to identity theft or fraud:

- **Bank Fraud:** To engage in an act or pattern of activity where the purpose is to defraud a bank of funds.
- **Blackmail:** A demand for money or other consideration under threat to do bodily harm, to injure property, to accuse of a crime, or to expose secrets.
- **Bribery:** When money, goods, services, information or anything else of value is offered with intent to influence the actions, opinions, or decisions of the taker. You may be charged with bribery whether you offer the bribe or accept it.
- **Computer fraud:** Where computer hackers steal information sources contained on computers such as: bank information, credit cards, and proprietary information.
- **Credit Card Fraud:** The unauthorized use of a credit card to obtain goods of value.
- **Extortion:** Occurs when one person illegally obtains property from another by actual or threatened force, fear, or violence, or under cover of official right.
- **Forgery:** When a person passes a false or worthless instrument such as a check or counterfeit security with the intent to defraud or injure the recipient.
- **Health Care Fraud:** Where an unlicensed health care provider provides services under the guise of being licensed and obtains monetary benefit for the service.
- **Larceny/Theft:** When a person wrongfully takes another person's money or property with the intent to appropriate, convert or steal it.
- **Money Laundering:** The investment or transfer of money from racketeering, drug transactions or other embezzlement schemes so that it appears that its original source either cannot be traced or is legitimate.

- **Telemarketing Fraud:** Actors operate out of boiler rooms and place telephone calls to residences and corporations where the actor requests a donation to an alleged charitable organization or where the actor requests money up front or a credit card number up front, and does not use the donation for the stated purpose.
- **Welfare Fraud:** To engage in an act or acts where the purpose is to obtain benefits (i.e. Public Assistance, Food Stamps, or Medicaid) from the State or Federal Government.

### Reporting Security Incidents

These Security Standards and the associated HMIS Policies and Procedures are intended to prevent, to the greatest degree possible, any security incidents. However, should a security incident occur, the following procedures should be followed in reporting:

- Any HMIS End User who becomes aware of or suspects that HMIS system security and/or client privacy has been compromised must immediately report the concern to their Partner Agency Security Officer.
- In the event of a suspected security or privacy concern the Partner Agency Security Officer should complete an internal investigation. If the suspected security or privacy concern resulted from an End User's suspected or demonstrated noncompliance with the HMIS End User Agreement, the Partner Agency Security Officer should have the HMIS System Administrator deactivate the End User's User ID until the internal investigation has been completed.
- Following the internal investigation, the Partner Agency Security Officer shall notify the Lead Security Officer of any substantiated incidents that may have compromised HMIS system security and/or client privacy whether or not a release of client PPI is definitively known to have occurred. If the security or privacy concern resulted from demonstrated noncompliance by an End User with the HMIS End User Agreement, the Lead Security Officer reserves the right to permanently deactivate the User ID for the End User in question.
- Within one business day after the Lead Security Officer receives notice of the security or privacy concern, the Lead Security Officer and Partner Agency Security Officer will jointly establish an action plan to analyze the source of the security or privacy concern and actively prevent such future concerns. The action plan shall be implemented as soon as possible, and the total term of the plan must not exceed thirty (30) days.
- If the Partner Agency is not able to meet the terms of the action plan within the time allotted, the HMIS System Administrator, in consultation with the Sacramento County Continuum of Care Advisory Board, may elect to terminate the Partner Agency's access to HMIS. The Partner Agency may appeal to the CoC Advisory Board for reinstatement to HMIS following completion of the requirements of the action plan.
- In the event of a substantiated release of PPI in noncompliance with the provisions of these Security Standards, the Sacramento County HMIS Policies and Procedures, or the Partner Agency Privacy Statement, the Partner Agency Security Officer will make a reasonable attempt to notify all impacted individual(s). The Lead Security Officer must approve of the method of notification and the Partner Agency Security Officer must provide the Lead Security Officer with evidence of the Agency's notification attempt(s). If the Lead Security Officer is not satisfied with the Agency's efforts to notify impacted individuals, the Lead Security Officer will attempt to notify impacted individuals at the Agency's expense.
- The HMIS Lead Agency will notify the appropriate body of the Continuum of Care of any substantiated release of PPI in noncompliance with the provisions of these Security Standards, the HMIS Policies and Procedures, or the Partner Agency Privacy Statement.

- The HMIS Lead Agency will maintain a record of all substantiated releases of PPI in noncompliance with the provisions of these Security Standards, the Sacramento County HMIS Policies and Procedures, or the Partner Agency Privacy Statement for 7 years.
- The Continuum of Care reserves the right to permanently revoke a Partner Agency's access to HMIS for substantiated noncompliance with the provisions of these Security Standards, the Sacramento County HMIS Policies and Procedures, or the Partner Agency Privacy Statement that resulted in a release of PPI.

## Privacy and Security Monitoring

### New HMIS Partner Agency Site Security Assessment

- Prior to establishing access to HMIS for a new Partner Agency, the Lead Security Officer will assess the security measures in place at the Partner Agency to protect client data (see Technical Safeguards – Workstation Security). The Lead Security Officer or other HMIS System Administrator will meet with the Partner Agency Executive Director (or executive-level designee) and Partner Agency Security Officer to review the Partner Agency's information security protocols prior to countersigning the HMIS Memorandum of Understanding. This security review shall in no way reduce the Partner Agency's responsibility for information security, which is the full and complete responsibility of the Partner Agency, its Executive Director, and its HMIS Agency Security Officer.

### Semiannual Partner Agency Self-Audits

- The Partner Agency Security Officer will use the Compliance Certification Checklist to conduct semiannually security audits of all Partner Agency HMIS End User workstations.
- The Partner Agency Security Officer will audit for inappropriate remote access by End-Users by associating User login date/times with employee time sheets. End Users must certify that they will not remotely access HMIS from a workstation (ie: personal computer) that is not subject to the Partner Agency Security Officer's regular audits.
- If areas are identified that require action due to noncompliance with these standards or any element of the Sacramento County HMIS Policies and Procedures, the Partner Agency Security Officer will note these on the Checklist, and the Partner Agency Security Officer and/or HMIS Agency Administrator will work to resolve the action item(s) within 15 days.
- Any Checklist that includes 1 or more findings of noncompliance and/or action items will not be considered complete until all action items have been resolved. The findings, action items, and resolution summary must be reviewed and signed by the Agency's Executive Director or other empowered officer prior to being forwarded to the Lead Security Officer.
- The Partner Agency Security Officer must turn in a copy of the Checklist to the Lead Security Officer on a semiannual basis.

### Annual Security Audits

- The Lead Security Officer will schedule the annual security audit in advance with the Partner Agency Security Officer.
- The Lead Security Officer will use the Compliance Certification Checklist to conduct security audits.
- The Lead Security Officer must randomly audit at least 10% of the workstations used for HMIS data entry for each HMIS Partner Agency. In the event that an agency has more than 1 project site, at least 1 workstation per project site must be audited.

- If areas are identified that require action due to noncompliance with these standards or any element of the Sacramento County HMIS Policies and Procedures, the Lead Security Officer will note these on the Checklist, and the Partner Agency Security Officer and/or HMIS Agency Administrator will work to resolve the action item(s) within 15 days.
- Any Checklist that includes 1 or more findings of noncompliance and/or action items will not be considered complete until all action items have been resolved and the findings, action items, and resolution summary has been reviewed and signed by the Agency's Executive Director or other empowered officer and forwarded to the HMIS Lead Security Officer.

SACRAMENTO
STEPS FORWARD
Ending Homelessness. Starting Fresh.

# HMIS PRIVACY STATEMENT

## Sacramento CoC Homeless Management Information System

## Full Notice

## Version 1.0

## I. What This Notice Covers

A. This notice describes the Homeless Management Information System (HMIS) privacy policy and practices of Agency's Name). Our main office is located at Agency's Address.

B. The policy and practices in this notice covers the collection, use and maintenance of protected personal information for persons served by Agency's Name, as an organization affiliated with the Sacramento Continuum of Care (CoC). If this agency is a covered entity under HIPAA, you may have additional rights regarding your protected health information and these rights will be described to you in the agency's Policy of Privacy Practices under HIPAA.

C. Personally Identifiable Information / Protected Personal information (hereby known as PPI) is any information we maintain about a client that:

1. allows identification of an individual directly or indirectly;

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 client.

D. We adopted this policy because of the U.S. Department of Housing and Urban Development (HUD) issued standards for Homeless Management Information Systems. We intend our policy and practices to be consistent with those standards. See 69 Federal Register 45888 (July 30, 2004).

E. This notice informs our clients, our staff, and others how we process personal information. We follow the policy and practices described in this notice.

F. We may amend this notice and our policy or practices at any time. Amendments may affect personal information that we obtained before the effective date of the amendment.

1. Amendments to this privacy statement will be approved by the HMIS System Administrator.

G. We give a written copy of this privacy statement to any individual who asks.

## II. How and Why We Collect Personal Information

A. We collect PPI only when appropriate to provide services or for another specific purpose of our organization or when required by law. We may collect information for these purposes:

1. to provide or coordinate services to clients;
2. to produce aggregate-level reports regarding use of services;
3. to track individual project-level outcomes;
4. to identify unfilled service needs and plan for the provision of new services;
5. to conduct research for consulting and/or educational purposes; and
6. to accomplish any and all other purposes deemed appropriate by the CoC.

B. We only use lawful and fair means to collect personal information.

C. We normally collect personal information with the knowledge or consent of our clients. If you seek our assistance and provide us with personal information, we assume that you consent to the collection of information as described in this notice.

D. We share this data with Sacramento Steps Forward (SSF); the agency appointed by the CoC to manage all personal information we record about our clients.

E. We post a Consumer Notice at our intake desk or other location explaining the reasons we ask for personal information. The Consumer Notice reads:

**This Agency receives funding from U.S. Department of Housing and Urban Development to provide services for homeless and near homeless individuals and their families. A requirement of this funding is that the Agency participates in the Sacramento Continuum of Care, Homeless Management Information System (HMIS), which collects basic information about consumers receiving services from this Agency. This requirement was enacted in order to get a more accurate count of individuals and families who are homeless, and to identify the need for different services.**

**We only collect information that we consider to be appropriate. The collection and use of all personal information is guided by strict standards of confidentiality. A copy of our Privacy Notice describing our privacy practice is available to all consumers upon request. Agencies participating in HMIS share information with local agencies partnered in HMIS unless they serve a protected population, in compliance with applicable federal and state law. The list of HMIS Partner Agencies is available to consumers at intake upon request. Sharing information among agencies allows those agencies to work in a cooperative manner to provide you with better services.**

**You have the right to refuse certain data answers to be entered into the HMIS database. As such, we request every consumer whom we serve to sign a "Consumers Informed Consent & Release of Information Authorization". Although you will receive services if you refuse to provide data answers, your eligibility to receive some specialized services may be impacted by not participating in HMIS.**

**You do have the ability to share your personal information with other area agencies that participate in the network by completing a "Consumers Informed Consent & Release of Information Authorization" form. This will allow those agencies to work in a cooperative manner to provide you with efficient and effective services.**

## III. How We Use and Disclose Personal Information

A. We use or disclose personal information for activities described in this part of the statement. We may or may not make any of these uses or disclosures with your information. We assume that you consent to the use or disclosure of your personal information for the purposes described below and for other uses and disclosures that we determine to be compatible with these uses or disclosures:

1. to provide or coordinate services to individuals; data may be shared with other HMIS participating agencies (a copy of participating agencies can be found at www.sacramentostepsforward.org);
2. for functions related to payment or reimbursement for services;
3. to carry out administrative functions such as legal, audits, personnel, oversight, and management functions;
4. to create de-identified (anonymous) information that can be used for research and statistical purposes without identifying clients
5. when required by law to the extent that use or disclosure complies with and is limited to the requirements of the law;
6. to avert a serious threat to health or safety if;
   a. we believe that the use or disclosure is necessary to prevent or lessen a serious imminent threat to the health or safety of an individual or the public; **and**
   b. the use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat.
7. to report about an individual we reasonably believe to be a victim of abuse, neglect or domestic violence to a governmental authority (including a social service or protective services agency) authorized by law to receive reports of abuse, neglect or domestic violence in any of the following three (3) circumstances:
   a. where the disclosure is required by law and the disclosure complies with and is limited to the requirements of the law;
   b. if the individual agrees to the disclosure; **or**
   c. to the extent that the disclosure is expressly authorized by statute or regulation, and either of the following are applicable:
      i. we believe the disclosure is necessary to prevent serious harm to the individual or other potential victims; **or**
      ii. if the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the personal information for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

   When we make a permitted disclosure about a victim of abuse, neglect or domestic violence, we will promptly inform the individual who is the victim that a disclosure has been, or will be, made except if:

   a. we, in the exercise of professional judgment, believe informing the individual would place the individual at risk of serious harm; **or**
   b. we would be informing a personal representative (such as a family member or friend), and we reasonably believe the personal representative is responsible for the abuse, neglect or other injury, and that informing the personal representative would not be in the best interests of the individual as we determine in the exercise of professional judgment.
8. to a law enforcement official for a law enforcement purpose (if consistent with

applicable law and standards of ethical conduct) under any of these circumstances:

a. in response to a lawful court order, court-ordered warrant, subpoena or summons issued by a judicial officer, or a grand jury subpoena;

b. if the law enforcement official makes a written request for personal information that:

  i. is signed by a supervisory official of the law enforcement agency seeking the personal information;

  ii. states that the information is relevant and material to a legitimate law enforcement investigation;

  iii. identifies the personal information sought;

  iv. is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; **and**

  v. states that de-identified information could not be used to accomplish the purpose of the disclosure.

c. if we believe in good faith that the personal information constitutes evidence of criminal conduct that occurred on our premises

d. In response to an oral request for the purpose of identifying or locating a suspect, fugitive, material witness or missing person. In these cases the ONLY personal information that may be shared is ~~and the personal information disclosed consists only of~~ the name, address, date of birth, place of birth, Social Security Number, and distinguishing physical characteristics of the individual. No programmatic information including program enrollments, services provided, field contacts, or the like may be shared; **or**

e. if:

  i. the official is an authorized federal official seeking personal information for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879 (threats against the President and others); **and**

  ii. the information requested is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought.

9. to comply with government reporting obligations for HMIS and for oversight of compliance with the HMIS requirements.

B. Before we make any use or disclosure of your personal information that is not described here, we seek your consent first.

## IV. How to Inspect and Correct Personal Information

A. You may inspect and have a copy of your personal information that we maintain. We will offer to explain any information that you may not understand.

B. We will consider a request from you for correction of inaccurate or incomplete personal information that we maintain about you. If we agree that the information is inaccurate or incomplete, we may delete it or we may choose to mark it as inaccurate or incomplete and to supplement it with additional information.

C. We may deny your request for inspection or copying of personal information if:

1. the information was compiled in reasonable anticipation of litigation or comparable

proceedings;

2. the information is about another individual (other than a health care provider or homeless provider);
3. the information was obtained under a promise or confidentiality (other than a promise from a health care provider or homeless provider) and if the disclosure would reveal the source of the information; **or**
4. disclosure of the information would be reasonably likely to endanger the life or physical safety of any individual.

D. If we deny a request for access or correction, we will explain the reason for the denial. We will also include, as part of the personal information that we maintain, documentation of the request and the reason for the denial

E. We may reject repeated or harassing requests for access to or correction of personal information.

## V. Data Retention

A. We collect only personal information that is relevant to the purposes for which we plan to use it. To the extent necessary for those purposes, we seek to maintain only personal information that is accurate, complete, and timely.

B. We will dispose of personal information not in current use seven (7) years after the information was created or last changed. As an alternative to disposal, we may choose to remove identifiers from the information.

C. We may keep information for a longer period if required to do so by an applicable statute, regulation, contract, or other requirement.

## VI. Complaints and Accountability

A. We accept and consider questions or complaints about our privacy and security policies and practices.

1. Any questions or complaints regarding our privacy and security policies and practices should be addressed to the following:

   HMIS Site Administrator, [Agency name and address and phone number].

   The HMIS Site Administrator will respond in writing within 30 days to the question or complaint.

   a. If the response from the HMIS Site Administrator is unsatisfactory, your original questions and/or complaints, along with the response from the HMIS Site Administrator, should be forwarded to the HMIS System Administrator, 1331 Garden Highway, Suite 100, Sacramento CA 95833. The HMIS System Administrator will respond in writing within 30 days to the question or complaint.

B. All members of our staff (including employees, volunteers, affiliates, contractors and associates) are required to comply with this privacy Policy. Each staff member must receive and acknowledge receipt of a copy of this privacy statement.

## VII. Privacy Policy Change History

A. Version 1.0, Effective January 1st, 2016, Original Version d

# SACRAMENTO HOMELESS MANAGEMENT INFORMATION SYSTEM: DATA QUALITY PLAN

Adopted 08.12.15

# Contents

## Introduction

This document describes the Homeless Management Information System (HMIS) Data Quality Plan for the Sacramento Continuum of Care (CoC). The Plan includes data quality standards and protocols for ongoing data quality monitoring that meets requirements set forth by the US Department of Housing and Urban Development (HUD). It has been developed by HMIS Lead Agency Sacramento Steps Forward, in coordination with the CoC Advisory Board's HMIS & Data Committee, for approval by the Advisory Board. This Data Quality Plan will be updated annually, considering the latest HMIS Data Standards and locally developed performance plans.

The HMIS is Sacramento's electronic data collection system that maintains client-level data about the individuals and families who receive homeless and other human services throughout the community. The HMIS also assists agencies with project administration, operations, and reporting. Some of the typical benefits of an HMIS include:

- Improved service delivery and prompt referrals for clients
- Immediate access to important client information
- Quick and easy preparation of reports for funders, stakeholders
- Access to CoC-level performance data to inform system improvements

HUD requires that all CoCs receiving HUD grants utilize HMIS or similar database. The County of Sacramento also requires that all projects receiving CalWORKS and other County funding must report client-level data in HMIS. All VA-funded Grant Per Diem and Supportive Services for Veteran Families (SSVF) projects must also report client-level data in HMIS. The only current exceptions to these funders' requirements are projects and agencies specifically serving victims of domestic violence.

## What is a Data Quality Plan?

A data quality plan is a community-level document that enhances the ability of the CoC to achieve statistically valid and reliable data. A data quality plan sets expectations for the CoC, the HMIS Lead Agency, and the end users to capture valid and reliable data on persons accessing the homeless assistance system.

Developed by the HMIS Lead Agency and formally adopted by the CoC, the plan:

- Identifies the responsibilities of all parties within the CoC with respect to data quality;
- Establishes specific data quality benchmarks for timeliness, completeness, accuracy, and consistency;
- Describes the procedures for implementing the plan and monitoring progress toward meeting data quality benchmarks; and
- Establishes timelines for monitoring data quality on a regular basis.

## HMIS Data Standards

In May of 2014, HUD published the revised and final HMIS Data Standards. The May 2014 Data Standards replaced the March 2010 HMIS Data Standards by which client and project-level data reporting have been guided. The HMIS Data Standards identify Universal Data Elements, Program Specific Data Elements, and Project Descriptor Data Elements which are required of all homeless projects participating in the HMIS. Frequency of data collection and subsequent entry into the HMIS are also required.

## Universal Data Elements

The Universal Data Elements establish the baseline data collection requirements for all homeless housing and/or service providers entering data into the HMIS. They are the basis for producing unduplicated estimates of the number of homeless people accessing services from homeless assistance providers, basic demographic characteristics of people who are homeless, and patterns of service use, including information on shelter stays and homelessness episodes over time.

The required Universal Data Elements include the following:

3.1 Name
3.2 Social Security Number
3.3 Date of Birth
3.4 Race
3.5 Ethnicity
3.6 Gender
3.7 Veteran Status
3.8 Disabling Condition
3.9 Residence Prior to Project Entry
3.10 Project Entry Date
3.11 Project Exit Date
3.12 Destination
3.13 Personal ID
3.14 Household ID
3.15 Relationship to Head of Household
3.16 Client Location
3.17 Length of Time on Street, in an ES or Safe Haven

## Program Specific Data Elements

Program-Specific Data elements provide information about the characteristics of clients, the services that are provided, and client outcomes. Many of these data elements represent transactions or information that may change over time. Most Program Specific Data Elements shall be captured at project entry and exit, and a few must be captured at project entry, exit, and on an annual basis.

The required Program Specific Data Elements include the following:

4.1 Housing Status
4.2 Income and Sources
4.3 Non-Cash Benefits
4.4 Health Insurance
4.5 Physical Disability
4.6 Developmental Disability
4.7 Chronic Health Condition
4.8 HIV/AIDS
4.9 Mental Health Problem
4.10 Substance Abuse
4.11 Domestic Violence
4.12 Contact
4.13 Date of Engagement
4.14 Services Provided
4.15 Financial Assistance Provided
4.16 Referrals Provided
4.17 Residential Move-In Date
4.18 Housing Assessment Disposition
4.19 Housing Assessment at Exit

## Project Descriptor Data Elements

Project Descriptor Data Elements (PDDEs) contain basic information about projects participating in a CoC's HMIS and help ensure the HMIS is the central repository of information about homelessness. The PDDE's are the building blocks of the HMIS. They enable the HMIS to:

1. Associate client-level records with the various projects that client will enroll in across CoC projects;
2. Clearly define the type of project the client is associated with the entire time they received housing or services;
3. Identify which federal partner programs are providing funding to the project; and
4. Track bed and unit inventory and other information, by project, which is relevant for the Annual Homeless Assessment Report (AHAR), system performance measures, Housing Inventory Counts (HIC), Point In Time (PIT) counts, and bed utilization reporting.

Project descriptor data are generally entered and managed by the HMIS Lead Agency, not a project end user. They are created at initial project setup within the HMIS and shall be reviewed at least once annually and updated as needed.

The required Project Descriptor Data Elements include the following:

2.1 Organization Identifiers
2.2 Project Identifiers
2.3 Continuum of Care Code
2.4 Project Type
2.5 Method for Tracking Emergency Shelter
2.6 Federal Partner Funding Sources
2.7 Bed and Unit Inventory Information
2.8 Site Information - Optional
2.9 Target Population

## Benchmarks and Goals

## Timeliness

Timeliness answers the question: "Is the necessary client information entered into HMIS within a reasonable period of time?"

When data is entered in a timely manner, it helps reduce human error that can occur when too much time has elapsed between the data collection/service transaction and the data entry. Timely data entry also ensures that the data is accessible when it is needed, whether for monitoring purposes, meeting funding requirements, or for responding to requests for information. Live Data Entry is highly recommended. There is a Timeliness Report that agencies can use under "Project Based Reports" to monitor the timeliness of data entry for entry into a project and exit from a project.

Each type of project has different expectations on timely data entry. Timeliness is measured by comparing the enrollment entry/exit date to the assessment entry/exit created date. Timeliness cannot be edited, only improved going forward – but assessment information dates should match the date the client interview occurred.

## Data Entry Timeline by Project Type

All data shall be entered into the HMIS in a timely manner and Sacramento CoC's goal is to enter 100% of data per the following data entry timelines. As the COC recognizes entering 100% of all data may not be possible in all cases, a benchmark of 95% of all clients being entered in the following time frames has been established.

- **Emergency Shelter projects for Singles:** All Universal Data Elements and Project Specific Data Elements must be entered within **48 hours** of intake and/or exit.
- **Emergency Shelter projects for Families:** All Universal Data Elements and Project Specific Data Elements must be entered within **48 hours** of intake and/or exit.
- **Transitional Housing and Permanent Housing projects**: All Universal Data Elements and Project Specific Data Elements must be entered within **three (3) days** of intake and/or exit.
- **Permanent Supportive Housing (PSH):** All Universal Data Elements and Project Specific Data Elements must be entered within **three (3) days** of intake and/or exit.
- **Prevention and Rapid Re-Housing projects:** All Universal Data Elements and Project Specific Data Elements must be entered within **three (3) days** of intake and/or exit.
- **Supportive Service Only projects (SSO):** All Universal Data Elements and Project Specific Data Elements must be entered within **three (3) days** of intake and/or exit.

Program Descriptor Data Elements for all program types (Emergency Shelter, Transitional Housing, Permanent Housing, Prevention and Rapid Re-Housing, and Supportive Service Only programs) shall be entered concurrently with setup of the program in the Sacramento HMIS.

## Completeness

Completeness answers the question: "Are all of the clients we serve being entered into HMIS? Are all of the necessary data elements being recorded into HMIS?"

Complete data is the key to assisting clients in finding the right services and benefits to end their homelessness. Incomplete data may hinder an organization's ability to provide comprehensive care to the clients it serves. Incomplete data can also negatively impact both the Sacramento Continuum of Care and Sacramento Steps Forward's ability to make generalizations of the population it serves, track patterns in client information and changes within the homeless population, and adapt strategies appropriately. HMIS data quality is also part of funding applications, including CoC and ESG, and low HMIS data quality scores may impact renewal funding as well as future funding requests.

Complete data facilitates confident reporting and analysis on the nature and extent of homelessness, including:

- Unduplicated counts of persons served;

- Patterns of use of persons entering and exiting the homeless assistance system in the community; and

- Evaluation of the effectiveness of the community's homeless assistance system.

## Completeness – Universal and Program Specific Data Elements

Sacramento CoC's goal is to collect 100% of all data elements (**Universal and Program Specific**). Though the CoC recognizes that collecting 100% of all data elements may not be possible in all cases, this goal is set in order to guarantee that the CoC continues to meet HUD-funding compliance requirements and to further ensure participation by the CoC in the Annual Homeless Assessment Report (AHAR). Therefore, the Sacramento CoC's HMIS & Data Committee with the CoC Board's approval, has established Data Quality Thresholds (see Table 1, Appendix A). The Data Quality Thresholds set an acceptable range of "Missing/Data Not Collected", and "Client Doesn't Know/Client Refused" responses, depending on the data element. To determine compliance, percentages will be rounded (example: .04% becomes 0%).

HUD/Sacramento CoC expects that all clients receiving housing and/or services through the homeless assistance system will have their service delivery documented in the HMIS. If a project only enters data on a few of its clients, the project's efficiency cannot accurately be determined. Incomplete data may erroneously reflect low bed utilization rates (for housing projects), and may inaccurately reflect clients' progress in meeting programmatic goals (i.e. employment, transitioning to permanent housing). All projects using the HMIS shall enter data on one hundred percent (100%) of the clients they serve. Due to a lack of historical data, these standards will be reviewed and revised annually to make sure the thresholds are reasonable.

## Completeness – Project Descriptor Data Elements

Pursuant to HUD's HMIS Data Standards, all Project Descriptor Data Elements must be entered for all projects participating in the HMIS. In order to ensure that the CoC meets HUD-funding compliance requirements, the following acceptable response rate ranges have been established:

| Project Descriptor Data Elements | TARGET % | ACCEPTABLE NULL/MISSING % |
|---|---|---|
| 2.1 Organization Identifiers | 100% | 0% |
| 2.2 Project Identifiers | 100% | 0% |
| 2.3 Continuum of Care Code | 100% | 0% |
| 2.4 Project Type | 100% | 0% |
| 2.5 Method for Tracking Emergency Shelter Utilization | 100% | 0% |
| 2.6 Federal Partner Funding Sources | 100% | 0% |
| 2.7 Bed and Unit Inventory Information | 100% | 0% |
| 2.8 Site Information – Optional | 100% | 0% |
| 2.9 Target Population | 100% | 0% |

## Bed/Unit Utilization Rates

One of the primary features of the HMIS is its ability to record the number of client stays (bed nights) at a homeless residential facility. A project's bed/unit utilization rate is the number of beds/unit occupied as a percentage of the entire bed inventory. When a client is admitted into a residential project (emergency, transitional, or permanent), s/he is assigned a housing service. This housing service is named as "Housed with------name of the project or funding source". The client remains in this service until s/he is discharged from the project. When the client is discharged from the project, s/he is also discharged from this housing service in the HMIS.

Acceptable range of bed/unit utilization rates for established projects (as per AHAR Guidelines):

- Emergency Shelters: 65%-105%
- Transitional Housing: 65%-105%
- Permanent Supportive Housing: 65%-105%

A project's bed utilization rate is an excellent barometer of data quality. A low utilization rate could reflect low occupancy, but it could also indicate that data is not being entered in the Sacramento HMIS for every client served. A high utilization rate could reflect that the project is over capacity, but it could also indicate that clients have not been properly discharged from the project in the Sacramento HMIS.

## Housing Inventory

The CoC Lead Agency will request housing inventory from each residential facility in the homeless assistance system at least annually. The homeless assistance provider operating the residential facility will provide its housing inventory when requested or when housing inventory has changed to the CoC Lead Agency in timely manner to ensure updates in HMIS.

The CoC recognizes that new projects may require time to reach the projected occupancy numbers and will not expect them to meet the utilization rate requirement during the **first six months** of operating.

## Accuracy

Accuracy answers the question: "Does HMIS data accurately reflect true client information? Are the necessary data elements being recorded in HMIS in a consistent manner?"

Information entered into the HMIS needs to be valid, i.e. it needs to accurately represent information on the people that enter any of the homeless service projects contributing data to the HMIS. The best way to measure accuracy of client data is to compare the HMIS information with more accurate sources, such as a social security card, birth certificate, or driver's license. To ensure the most up-to-date and complete data, data entry errors should be corrected on a monthly basis.

As a general rule, it is a better practice to select "client doesn't know/refused" than to misrepresent the population.

Data consistency will ensure that data is understood, collected, and entered consistently across all projects in the HMIS. Consistency directly affects the accuracy of data; if an end user collects all of the data, but they don't collect it in a consistent manner, then the data may not be accurate. All data in HMIS shall be collected and entered in a common and consistent manner across all projects. To that end, all intake and data entry workers will complete an initial training before accessing the live HMIS system, and access additional training opportunities offered by the HMIS Administrator.

All Universal Data Elements and Program Specific Data Elements must be obtained from each adult and unaccompanied youth who apply for services through the homeless assistance system. Most Universal Data Elements are also required for children age 17 years and under.

Most Universal Data Elements and Program Specific Data Elements include a 'Client doesn't know' or 'Client refused' response category. These are considered valid responses if the client does not know or the client refuses to respond to the question. It is not the intention of the federal partners that clients be denied assistance if they refuse or are unable to supply the information. However, some information may be required by projects or public or private funders to determine eligibility for housing or services, or to assess needed services. The 'Client doesn't know' or 'Client refused' responses shall not be used to indicate that the case manager or data entry person does not know the client's response. The HMIS Data Standards assume that fields for which data are not collected will be left blank (i.e. 'missing'). Since Sacramento's HMIS system requires a response to all data fields before saving a record, the HMIS User must use a specific response category "Data not collected". In such cases, "Data not collected" response category is treated as missing data for reporting purposes.

## Data Consistency Checks

The HMIS staff will check data accuracy and consistency by running reports that check for entry errors such as duplicate files created, overlapping enrollments, or inconsistent responses. Examples of these checks will include:

1. Verification that new client profiles do not duplicate existing profiles
2. Verification that information describing a client's experience in homelessness conforms with other components of the clients record (e.g. a client's approximate date of start of homelessness cannot be AFTER a program enrollment)
3. Verification the referrals and referral responses are correctly entered.
4. Verification that housing start dates are entered correctly.

~~The HMIS staff may check data accuracy and consistency by running reports that check for entry errors such as duplicate files created, overlapping enrollments, or inconsistent assessment responses.~~

## Data Quality Monitoring Plan

The purpose of monitoring is to ensure that the agreed-upon data quality targets are met to the greatest extent possible, and that data quality issues are quickly identified and resolved. The CoC recognizes that the data produced from the HMIS is critical to meet the reporting and compliance requirements of HUD, the individual agencies, and the CoC as a whole.

The HMIS administer will post quarterly dashboards reporting program-level performance concerning meeting data quality goals. The reports will include the standards laid out in the Data Quality Plan and will also include other data quality issues as determined by the HMIS Administrator. These public reports will not identify specific programs, but agencies will be able to identify their own data.

# Roles and Responsibilities

## HMIS Administrator

The HMIS Administrator is responsible for building reports and making them available to the CoC. This includes the data quality reports necessary for data correction. The HMIS staff will be responsible for the ongoing maintenance of existing reports as well, which includes changes in reports as updates are made to the system.

The HMIS team at Sacramento Steps Forward is also responsible for providing the necessary training for the CoC. Currently, the HMIS team offers the following trainings: New User training, Management Training, Report training, HMIS Security Training, Refresher Training (groups or one-on-one sessions). In addition, HMIS staff is available to provide technical assistance to users that need help correcting data entry errors.

On a quarterly basis, the HMIS staff will provide to the HMIS committee data quality reports for agencies funded by the CoC and offer additional training to those agencies that need to improve their data quality. The quarterly reports for the HMIS committee will provide information on timeliness, bed utilization rates, and data completeness for CoC-funded projects.

## HMIS & Data Committee

The HMIS & Data Committee is responsible for reviewing data quality reports quarterly and working with HMIS staff and providers to correct data that does not comply with community-wide standards as established in the Data Quality Plan. The HMIS & Data Committee will maintain an ongoing relationship with the HMIS Administrator to identify training needs for the continuum based on monthly data quality reports.

# Data Review Timeline

Monitoring and data quality reviews will be conducted quarterly by the HMIS & Data Committee, in an annual cycle as follows:

| QUARTER | DATA UNDER REVIEW | TARGET REVIEW DATE |
|---|---|---|
| Quarter 1 | Months 1 - 3 Data | **25th of the 4th Month** |
| Quarter 2 | Month 4 - 6 Data | **25th of the 7th Month** |
| Quarter 3 | Month 7 - 9 Data | **25th of the 10th Month** |
| Quarter 4 | Month 10 - 12 Data | **25th of the 1st Month (New Cycle)** |

Additional monitoring, data quality and utilization rates reviews will be conducted in preparation for submission of AHAR data to HUD, in accordance with the following schedule:

| AHAR REVIEW MONTH | TARGET REVIEW DATE |
|---|---|
| October | **October 31st** |
| November | **November 30th** |
| December | **December 31st** |

| | |
|---|---|
| January | **January 31st** |
| February | **February 10th** |

## Target

When data quality benchmarks are met, reporting will be more reliable and can be used to evaluate service delivery, project design and effectiveness, and efficiency of the system. All HMIS partner agencies are expected to meet the data quality benchmarks described in this document. To achieve this, HMIS data will be monitored and reviewed in accordance with the schedule outlined in this section. All monitoring will be conducted by the Sacramento HMIS Lead Agency in accordance with the HMIS Data Quality Monitoring Tool (Design in Process), and with the full support of the CoC.

## Incentives and Enforcement

To ensure that HMIS partner agencies meet the minimum data entry standards set forth herein, a copy of this Data Quality Plan will be posted to the HMIS Lead's website. Sample intake, annual Status Assessment, and exit forms are posted on HMIS Lead's website. The HMIS Lead will provide data quality reports to HMIS partner agencies in accordance with the monitoring schedule described in the "Monitoring" section to facilitate compliance with the minimum data entry standards.

Agencies that meet the data quality benchmarks will be periodically recognized by the CoC. HMIS partner agencies that do not adhere to the minimum data entry standards set forth herein will be notified of their errors and provided with specific information regarding the nature of the inaccuracies and methods by which to correct them. The HMIS partner agencies will be given one month to correct any identified data quality issues. Training will be offered to agencies that remain noncompliant with the minimum data entry standards. HMIS partner agencies continuing in default may have access to the HMIS suspended until such time as agencies demonstrate that compliance with minimum data entry standards can be reached.

## Table 1, Appendix A

**Universal and Program Specific Data Element Quality Thresholds**

| **UNIVERSAL DATA ELEMENT** | **TARGET %** | **TH, PSH, HUD SSO, RRH, HP** | | **ES, Non-HUD SSO** | | **Outreach** | |
|---|---|---|---|---|---|---|---|
| | | Missing/ Data Not Collected | Client Doesn't Know/ Refused | Missing/ Data Not Collected | Client Doesn't Know/ Refused | Missing/ Data Not Collected | Client Doesn't Know/ Refused |
| 3.1 Name | 100% | 0% | 0% | 0% | 0% | 0% | 0% |
| 3.2 Social Security Number | 100% | 0% | 0% | 0% | 5% | 0% | 5% |
| 3.3 Date of Birth | 100% | 0% | 0% | 0% | 5% | 0% | 5% |
| 3.4 Race | 100% | 0% | 0% | 0% | 5% | 0% | 5% |
| 3.5 Ethnicity | 100% | 0% | 0% | 0% | 5% | 0% | 5% |
| 3.6 Gender | 100% | 0% | 0% | 0% | 0% | 0% | 0% |
| 3.7 Veteran Status | 100% | 0% | 0% | 0% | 5% | 0% | 5% |
| 3.8 Disabling Condition | 100% | 0% | 0% | 0% | 5% | 0% | 5% |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 3.9 Residence Prior to Project Entry | 100% | 0% | 0% | 0% | 0% | 0% | 0% |
| 3.10 Project Entry Date | 100% | 0% | 0% | 0% | 0% | 0% | 0% |
| 3.11 Project Exit Date | 100% | 0% | 0% | 0% | 0% | 0% | 0% |
| 3.12 Destination | 100% | 5% | 5% | 5% | 5% | 15% | 5% |
| 3.15 Relationship to Head of Household | 100% | 0% | 0% | 0% | 0% | 0% | 0% |
| 3.16 Client Location | 100% | 0% | 0% | 0% | 0% | 0% | 0% |
| 3.17 Length of Time on Street or in an Emergency Shelter | 100% | 0% | 0% | 0% | 0% | 0% | 0% |

| **PROGRAM SPECIFIC DATA ELEMENT** | **TARGET %** | **TH, PSH, HUD SSO, RRH, HP** | | **ES, Non-HUD SSO** | | **Outreach** | |
|---|---|---|---|---|---|---|---|
| | | Missing/ Data Not Collected | Client Doesn’t Know /Refused | Missing/ Data Not Collected | Client Doesn’t Know /Refused | Missing/ Data Not Collected | Client Doesn’t Know /Refused |
| 4.1 Housing Status | 100% | 0% | 0% | 0% | 0% | 0% | 0% |
| 4.2 Income and Sources | 100% | 0% | 0% | 0% | 0% | 0% | 0% |
| 4.3 Non-Cash Benefits | 100% | 0% | 0% | 0% | 0% | 0% | 0% |
| 4.4 Health Insurance | 100% | 0% | 0% | 0% | 0% | 0% | 0% |
| 4.5 Physical Disability | 100% | 0% | 0% | 0% | 0% | 0% | 0% |
| 4.6 Developmental Disability | 100% | 0% | 0% | 0% | 0% | 0% | 0% |
| 4.7 Chronic Health Condition | 100% | 0% | 0% | 0% | 0% | 0% | 0% |
| 4.8 HIV/AIDS | 100% | 0% | 0% | 0% | 0% | 0% | 0% |
| 4.9 Mental Health Problem | 100% | 0% | 0% | 0% | 0% | 0% | 0% |
| 4.10 Substance Abuse | 100% | 0% | 0% | 0% | 0% | 0% | 0% |
| 4.11 Domestic Violence | 100% | 0% | 0% | 0% | 0% | 0% | 0% |
| 4.12 Contact | 100% | | | | | 0% | 0% |
| Employed | 100% | 0% | 0% | 5% | 5% | 5% | 5% |

SACRAMENTO
STEPS FORWARD

# Annual HMIS User Recertification

HMIS users are required by the Sacramento CoC’s HMIS and Data Committee to be recertified each year. Recertification will be granted in one of two ways. First, HMIS users who score 70% or higher on the recertification quiz will be considered recertified. Alternatively, users may attend a monthly HMIS users training.

The quiz is open book. Users may refer to the user’s manual and the Bitfocus help site (get.clarityhs.help). Quiz takers, however, should not receive any help from individuals.

1. When is it permissible to share a client’s personal information with an outside source (check all correct answers)
    a. Never
    b. When presented with a subpoena
    c. As long as they working to help the client
    d. If the client provides explicit permission
    e. When the requests comes from a law enforcement officer

2. If a client declines to sign a release of information consent form, you should
    a. Not create a profile in the HMIS
    b. Create a profile but use an alias for their name
    c. Create a profile that is de-identified
    d. Ensure that the client’s Social Security number is not included in the profile

3. Sharing your HMIS access credentials is permissible when
    a. The other uses is working on your secure work computer
    b. The other user will only access the HMIS once and you change your password immediately after the use
    c. When you are sharing duties with co-workers to enroll clients
    d. Never

4. When searching for a client in the HMIS good practice includes (choose all that apply)
    a. Include as much information as is know about the client
    b. Search on the final four digits of the client’s Social Security Number
    c. Include at least their full first and last name
    d. Include the first three letters of their first and last names

5. Your agency needs to review a list of all of the client you were serving during the month of June. Which of these Clarity reports would be most appropriate for gathering that information?
    a. Annual Performance Review [HUDX-227-AD]
    b. Housing Census [Program Based] [HSNG-108]
    c. The Client List [GNRL-102]
    d. Program Roster [GNRL-106]
    e. User Activity Report [STFF-101]

6. When searching for a client, you find two entries that are similar to your client but each record differs on some counts. In one record the Social Security number is missing while your client does have a SSN. In another record the client has the same SSN, but the last name is spelled differently. What should you do to enroll your client in a new program?
    a. Assume that clients must be different because their data do not match perfectly. Create a new profile with the accurate data from your current client.
    b. Report the possibility of a duplicate record to the HMIS administrator
    c. Delete one of the two existing client profiles and enroll your client using the other profile.
    d. Enroll your client using the most similar record, and report the duplicate to the HMIS administrator

7. When adding a client profile to the HMIS, if a client provides several contradictory answer for their data of birth. What should be entered for the quality of the DOB
    a. Leave blank
    b. Data not collected
    c. Client doesn't know
    d. Client refused

8. Which of these procedures is NOT required to obtain client consent to collect data:
    a. Client must be provided a consent form.
    b. Client must be provided with a verbal explanation of the consent form
    c. Client must be briefed on how your agency agreement restricts the use of HMIS data
    d. Your Agency must post the HMIS Customer's Notice in a prominent place where clients may view it.

9. John Jay is exiting from a RRH program on July 8 of this year. He received 7 months of rent subsidies and is now exiting to a rental with no ongoing housing subsidy. You go to exit him and see that there is no housing move in date. What should be done?
   a. Enter the program exit date in the housing move in date field
   b. Enter the approximate date the client moved into subsidized housing in the move in date field
   c. Leave the field blank so to avoid back dating HMIS recored
   d. Check the client's program history and enter the date at which time rental subsidies began in the housing move in date field.

10. You are enrolling a family composed of a father (who is the HoH), an adult partner, and two children ages 11, and 17. Who should provide information for the enrollment?
    a. All family members should directly provide information separately
    b. The HoH should provide information for all family members
    c. The HoH should provide information for himself and the children. The Partner should provide information separately.
    d. The HoH should provide information for himself and the 11year old child. The partner and the 17 year old child should provide information separately.

11. The Jones family composed of a mother and her 2-year old daughter are enrolled in a RRH program. Later, the Mother's 12 year old son rejoins her. To enroll the son in the RRH program you should:
    a. Enroll the son separately as an unaccompanied youth
    b. Un-enroll the mother and 2-year old daughter from the program, and then enroll the complete family unit back into the program
    c. Find the correct program under the Head of Household's profile. Edit that program enrollment and add the 12 year old son through the program page.
    d. Enroll the son separately and then merge the family members together in the same group.

12. When should status or annual assessments be completed? (Check all correct answers)
    a. While they can be useful, they are never mandatory.
    b. Within 30 days of a clients one-year anniversary in a PSH project
    c. At the time of all significant changes in the client's status
    d. When a RRH client moves into a subsidized unit
    e. None to the above

13. You discover that a family unit that was served by one of your programs does not have anyone designated as the head-of-household. The family, however, has already exited the program. What should you do?
    a. Nothing. Once data has been entered into the system and a client has exited a program, the data should be left alone.
    b. Call the HMIS Program Administrator to delete the family's enrollment. Once deleted, a new enrollment with a proper head of household can be created and backdated.
    c. Correct the problem in the HMIS by undoing the exit for the client who should be the head of household (This is done by deleting the exit date). Then return to the program screen and edit the Head of Household icon.
    d. Keep a paper record of the error, and adjust program-level report when needed.

14. Sandy is a new client enrolling in an emergency shelter. She is 22 years old. For the last four months she has been sleeping on her friends' couches, and has never had an apartment or home of her own. Last night she got into a heated argument with her boyfriend and was kicked out of his apartment. What housing status should she be given on the Program enrollment screen?
    a. Category 1
    b. Category 2
    c. Category 3
    d. Category 4
    e. At-risk of homelessness
    f. Stably housed

**Other Topics to be reviewed**

1. Referral to the Community Queue
2. Moving a client enrollment from one program to another
3. Sources of help with HMIS questions
4. Account maintenance
5. Sharing HMIS data with law enforcement officials

SACRAMENTO STEPS FORWARD

# HMIS ANNUAL SECURITY CHECKLIST

Agency Name: ______________________________________________

Date of Audit: ______________________________________________

Agency Staff Member Completing Checklist: ___________________________

Agency Manager Responsible for Audit: ___________________________

- Using this Security Certification Checklist document, your agency must certify that it adheres to the Security Plan or provide a plan for remediation of non-compliant systems, including milestones to demonstrate elimination of the shortfall over time.
- Signatures indicate that agency understands of this audit and vouches for its results.
- Please communicate any security questions, requests, or security breaches to the HMIS Administrator.

| REQUIREMENT | ASSESSMENT | | | OUTCOME | FOLLOW-UP |
|---|---|---|---|---|---|
| **Agreements, Certifications & Licenses**<br>Does the Agency have all user agreements and certifications on file as well as agency related participation agreements and documentation? | Yes | No | | □ Action Needed<br>□ In Compliance | |
| | | | Does the agency have a signed copy of their most recent Agency Participation Agreement | | |
| | | | Does the agency have a designated HMIS contact person?<br>Name: | | |
| | | | All users have signed User License Agreements on file | | |
| | | | All users completed Privacy and Security Training (and have documentation of training) | | |
| | | | All users have completed applicable user training (and have documentation of training) | | |
| **Privacy: Posted HUD Public Notice**<br>Does the agency have a posted privacy notice in places visible to clients such as a lobby or intake rooms? | Yes | No | | □ Action Needed<br>□ In Compliance | |
| | | | Posted HUD Public Notice<br>Location: | | |

SACRAMENTO
STEPS FORWARD

| REQUIREMENT | ASSESSMENT | | | OUTCOME | FOLLOW-UP |
|---|---|---|---|---|---|
| **Privacy:**<br>**Privacy Notice**<br>Does the agency have a standard privacy notice? | Yes | No | | □ Action Needed<br>□ In Compliance | |
| | | | Does the agency use the standard CoC Privacy Notice? | | |
| | | | **OR** | | |
| | | | Does the agency notice have the following: | | |
| | | | • Specifies the purpose for collection of client information | | |
| | | | • Brief description of policies and procedures including vulnerable population protections. | | |
| | | | • Data collection, use and purpose limitations, including de-identified data | | |
| | | | • Client right to copy/inspect/correct record | | |
| | | | • The client compliant procedure | | |
| | | | • Notice to consumer that Privacy Notice may be updated over time and applies to all client info within the agency | | |
| | | | Copy obtained | | |
| | | | Privacy Notice is posted on the web at | | |
| **Privacy:**<br>**Hard Copy Data**<br>Does the agency protect hard copy data from unauthorized viewing or access? | Yes | No | | □ Action Needed<br>□ In Compliance | |
| | | | | | |
| | | | • Are paper files locked in a drawer/file cabinet | | |
| | | | • Are offices locked when not occupied | | |
| | | | • Are there any visible client files or reports on-site | | |

| REQUIREMENT | ASSESSMENT | | | OUTCOME | FOLLOW-UP |
|---|---|---|---|---|---|
| **Privacy:<br>Release of Information**<br>Does the agency use appropriate releases of information and are they consistent in collecting them with clients | Yes | No | | Action Needed<br>In Compliance | |
| | | | Agency collects ROI's from all intake clients | | |
| | | | Agency uses the CoC HMIS standardized ROI applicable to its level of sharing | | |
| | | | OR | | |
| | | | *(if using a modified ROI, review to make sure the following is included)* | | |
| | | | • A brief description of HMIS including a summary of the HUD Public Notice | | |
| | | | • A specific description of the Client Dashboard and an opportunity for the client to request that the screen be closed | | |
| | | | • A description of the agency's sharing partners (if any) and a description of what is shared | | |
| | | | • A specified end date on the release | | |
| | | | • Clients are presented with a copy of the agency privacy notice | | |
| | | | | | |
| **Privacy:<br>Special Considerations**<br>Does the agency have policies in place to assist with specific populations and special needs? | Yes | No | | Action Needed<br>In Compliance | |
| | | | Agency has a procedure to assist clients who are hearing impaired or do not speak English as a primary language. For example:<br>• Provisions for Braille or audio<br>• Available in multiple languages<br>• Available in large print | | |
| **Computer Systems: Virus Protection and System Updates**<br>Do all computers have virus protection with automatic updates? | Yes | No | | Action Needed<br>In Compliance | |
| | | | Verified through spot check of several computers | | |
| | | | Software and version: | | |
| | | | Date last update: | | |
| | | | OS updates are run regularly | | |

| | | | | | |
|---|---|---|---|---|---|
| **Computer Systems: Firewall**<br>Does the agency use a firewall to protect internal network servers and local user computers? | Yes | No | | Action Needed<br>In Compliance | |
| | | | **Single Computer** | | |
| | | | Individual workstation<br>Software and version: | | |
| | | | **Multiple (Networked) Computer Agencies:** | | |
| | | | Network firewall<br>Model and version: | | |
| **Computer Systems: Physical Access** | Yes | No | | Action Needed<br>In Compliance | |
| | | | All workstations in secured locations (locked offices) | | |
| | | | Workstations are logged off when not manned | | |
| | | | All workstations are password protected | | |
| | | | Computers used for data entry are not available to the general public, or connected to an open network/Wi-Fi connection (i.e. internet cafes, libraries, airports) | | |
| | | | A written plan for remote access exists if the agency permits users to access the system from outside the office. | | |
| **Data Collection**<br>Does the agency have consistent systematic processes for entering client data in the system? | Yes | No | | Action Needed<br>In Compliance | |
| | | | Agency has a procedure to ensure the First and Last Names and the DOB is accurate | | |
| | | | Agency is documenting the homeless status of clients at intake according to the reporting and eligibility guidelines issued by HUD | | |
| | | | All users have been trained on the definition of homelessness and its' application | | |
| | | | Income and non-cash benefits are being updated at least annually at exit | | |
| | | | If using paper, the intake data collection forms correctly align with the workflow | | |

| REQUIREMENT | ASSESSMENT | | | OUTCOME | FOLLOW-UP |
|---|---|---|---|---|---|
| **Data Collection**<br>(cont.) | Yes | No | | | |
| | | | 100% of clients are entered into the system within five (5) days of intake | | |
| | | | At minimum, all UDE's are collected. Data collected is appropriate for funding. | | |
| | | | Agencies are actively monitoring program participation and exiting clients. Clients are exited within 30 days of last contact unless program guidelines specify otherwise. | | |
| | | | Agencies are properly collecting discharge destinations | | |
| | | | Spot check of various random clients shows all required program information is being collected | | |
| **Data Quality Checks**<br>Agency staff regularly run reports to verify data quality and completeness. Staff correct data quality errors in a timely manner. | Yes | No | | Action Needed<br>In Compliance | |
| | | | Agency Security Officer/staff regularly run data quality reports | | |
| | | | Report frequency: | | |
| | | | Agencies are updating grant and program setups at least annually | | |
| | | | Staff regularly correct data entry errors and missing program elements | | |
| | | | Unexited client reports are monitored routinely | | |
| | | | Staff run outcome reports as applicable for program type (at least quarterly is recommended) | | |
| **Trainings and User Meetings**<br>Does the agency have regular trainings for users and regular meetings regarding HMIS issues? | Yes | No | | Action Needed<br>In Compliance | |
| | | | Agency has regular trainings and refresher meetings | | |
| | | | Agency has regular user meetings documented by meeting minutes (at least quarterly) | | |
| | | | Agency Security Officer/staff member have participated in Reports Training | | |
| | | | Agency representative participates in local committee meetings or forums as defined by the CoC | | |
| | | | Agency has a regular CQI process implemented to problem solve and monitor internal procedures and performance | | |

# HMIS Data Quality Report

CA-503: System

Report period 04/01/2018 - 06/30/2018

## Q1. Report Validation Table

Program Applicability: All Projects

| | |
|---|---|
| Total number of persons served | 9,191 |
| Number of adults (age 18 or over) | 6,864 |
| Number of children (under age 18) | 2,321 |
| Number of persons with unknown age | 6 |
| Number of leavers | 1,981 |
| Number of adult leavers | 1,315 |
| Number of adult and head of household leavers | 1,320 |
| Number of stayers | 7,210 |
| Number of adult stayers | 5,549 |
| Number of veterans | 870 |
| Number of chronically homeless persons | 2,782 |
| Number of youth under age 25 | 662 |
| Number of parenting youth under age 25 with children | 128 |
| Number of adult heads of household | 6,332 |
| Number of child and unknown-age heads of household | 35 |
| Heads of households and adult stayers in the project 365 days or more | 2,061 |

## Q2. Personally Identifiable Information (PII)

Program Applicability: All Projects

| Data Element | Client Doesnt Know/Refused | Information Missing | Data Issues | % of Error Rate |
|---|---|---|---|---|
| Name (3.1) | 4 | 220 | 6 | 2.5% |
| Social Security Number (3.2) | 194 | 34 | 161 | 4.23% |
| Date of Birth (3.3) | 5 | 34 | 9 | 0.52% |
| Race (3.4) | 49 | 36 | | 0.92% |
| Ethnicity (3.5) | 20 | 24 | | 0.48% |
| Gender (3.6) | 1 | 4 | | 0.05% |
| Overall Score | | | | 7.06% |

## Q3. Universal Data Elements

Program Applicability: All Projects

| Data Element | Error Count | % of Error Rate |
|---|---|---|
| Veteran Status (3.7) | 11 | 0.16% |
| Project Start Date (3.10) | 4 | 0.04% |
| Relationship to Head of Household (3.15) | 77 | 0.84% |
| Client Location (3.16) | 0 | 0% |
| Disabling Condition (3.8) | 1,006 | 10.95% |

## Q4. Income and Housing Data Quality

Program Applicability: All Projects

| Data Element | Error Count | % of Error Rate |
|---|---|---|
| Destination (3.12) | 474 | 23.92% |
| Income and Sources (4.2) at Start | 755 | 10.94% |
| Income and Sources (4.2) at Annual Assessment | 862 | 41.82% |
| Income and Sources (4.2) at Exit | 118 | 8.94% |
| Non-Cash Benefits (4.3) at Start | 822 | 11.91% |
| Non-Cash Benefits (4.3) at Annual Assessment | 879 | 42.65% |
| Non-Cash Benefits (4.3) at Exit | 130 | 9.85% |

## Q5. Chronic Homeless

Program Applicability: ES, SH, Street Outreach, TH & PH(All)

| Starting into project type | Count of total records | Missing time in institution (3.917.2) | Missing time in housing (3.917.2) | Approximate Date started (3.9.17.3)<br>**DK/R/missing** | Number of times (3.9.17.4)<br>**DK/R/missing** | Number of months (3.9.17.5)<br>**DK/R/missing** | % of records unable to calculate |
|---|---|---|---|---|---|---|---|
| ES, SH, Street Outreach | 2,611 | | | 2 | 122 | 492 | 19.69% |
| TH | 422 | 0 | 0 | 0 | 0 | 0 | 0% |
| PH (all) | 1,503 | 1 | 16 | 0 | 37 | 36 | 4.19% |
| Total | 4,536 | | | | | | 12.72% |

## Q6. Timeliness

Program Applicability: All Projects

| Time for Record Entry | Number of Project Start Records | Number of Project Exit Records |
|---|---|---|
| 0 days | 1,515 | 1,059 |
| 1-3 days | 509 | 393 |
| 4-6 days | 212 | 170 |
| 7-10 days | 108 | 104 |
| 11+ days | 215 | 256 |

## Q7. Inactive Records: Street Outreach and Emergency Shelter

Program Applicability: Street Outreach & ES-Night By Night

| Data Element | # of Records | # of Inactive Records | % of Inactive Records |
|---|---|---|---|
| Contact (Adults and Heads of Household in Street Outreach or ES-NbN) | 1,735 | 1,239 | 71.41% |
| Bed Night (All clients in ES-NbN) | 0 | 0 | 0% |

## Programs Included in Dataset

| Agency | Program Name |
|---|---|
| **Berkeley Food and Housing Project** | Roads Home |
| **Bishop Gallegos Maternity Home** | Bishop Gallegos Maternity Home |
| **City of Sacramento** | Winter Triage Shelter |
| **Community Against Sexual Harm** | CASH Center for Women |
| **Cottage Housing, Inc** | CH McClellan Park - HUD PSH (40) |
| **Cottage Housing, Inc** | CH McClellan Park - Non HUD PSH (43) |
| **Cottage Housing, Inc** | CH Quinn Cottages  - HUD PSH (70) |
| **Downtown Streets Team** | Sacramento Team |
| **El Hogar Community Service, Inc.** | Guest House Connections Lounge |
| **Family Promise of Sacramento** | Family Promise-HUD Rapid Re-Housing |
| **First Step Communities** | Pilgrimage Sacramento (Safe Ground) |
| **Flexible Supportive Rehousing Program (Sac County)** | Flexible Supportive Rehousing Program - GF |
| **Flexible Supportive Rehousing Program (Sac County)** | Flexible Supportive Rehousing Program - HCV |
| **Francis House Center - A Program of Next Move** | Family Rescue Program |
| **LifeSTEPS** | Shasta Hotel-Case Management |
| **Lutheran Social Services** | LSS Achieving Change Together (ACT) - HUD PSH (33) |
| **Lutheran Social Services** | LSS Building Bridges Program - HUD PSH |