Yolo County Homeless and Poverty Action Coalition (HPAC)

Homeless Management Information System (HMIS)
Policies and Procedures Manual

Davis/Woodland/Yolo County Continuum of Care (CA-521)

Adopted August 24, 2016

Table of Contents

Overview

Pursuant to 24 Code of Federal Regulations (CFR) Parts 91, 576, 580, and 583 Interim Rule[1], this document shall serve as the Homeless Management Information System (HMIS) Policies and Procedures Manual for the Davis/Woodland/Yolo County Continuum of Care (CA-521), hereafter known as the Homeless and Poverty Action Coalition (HPAC).

As a counterpart to HPAC's Policies and Procedures Manual, this document shall be reviewed, revised, and re-ratified every October with the general manual and governance charter upon a majority vote of all voting members present during the scheduled meeting.

Introduction

Given the volume of information included, the manual is divided into four sections:

- Section 1 describes HPAC's HMIS governance structure and the various roles and responsibilities of each entity
- Section 2 reviews several general operating policies and procedures such as how to add a user and how to request technical assistance
- Section 3 features HPAC's Data Quality Plan including local goals and benchmarks for timeliness, completeness, bed/unit utilization, bed coverage rates, and service-volume coverage rates
- Section 4 outlines HPAC's Security and Privacy Plan and the provisions in place to protect the privacy and security of the information collected and stored in HMIS

What is HMIS

HMIS is a local information technology system used to collect data on the provision of housing and services to persons and families experiencing homelessness as well as persons and families at risk of experiencing homelessness.

Who Uses HMIS

The U.S. Department of Housing and Urban Development (HUD) requires the use of HMIS for projects funded by the Continuum of Care (CoC) program, Emergency Solutions Grants (ESG) program, and Housing Opportunities for Persons with AIDS (HOPWA) program.

In 2010, the U.S. Interagency Council on Homelessness (USICH) affirmed HMIS as the official method of measuring outcomes in its Opening Doors: Federal Strategic Plan to Prevent and End Homelessness. Since then many federal agencies that provide homeless services funding have joined together and are working with HUD to coordinate the effort.

As of 2016, the U.S. Department of Veterans Affairs (VA) requires the use of HMIS for projects funded by the Supportive Service for Veteran Families (SSVF) program. The U.S. Department of Health and Human Services (HHS) requires the use of HMIS for projects funded by the Runaway and Homeless Youth (RHY) program and Projects for Assistance in Transition from Homelessness (PATH) program. In addition, many state and local government programs also require HMIS usage.

[1] 24 Code of Federal Regulations (CFR) Part 578 Continuum of Care Program Interim Rule: http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=&SID=5d030234903ffc25ad85a1fe4656bff7&mc=true&n=pt24.3.578&r=PART&ty=HTML#se24.3.578_165

An important exception to the aforementioned entities is victim service providers. Pursuant to 24 CFR Part 578.57[2], providers assisting victims of domestic violence, dating violence, human trafficking, sexual assault, and stalking victims are prohibited from using HMIS. Rather such providers must use a comparable database.

Why HMIS is Important

HMIS is a valuable resource because of its capacity to integrate and de-duplicate data across projects in a designated service area. Communities can use aggregate HMIS data to understand the size, characteristics, and needs of the homeless population at multiple levels: project, system, local, state, and national. The Annual Homeless Assessment Report (AHAR) is HUD's annual report that provides Congress with detailed data on individuals and families experiencing homelessness across the country each year. HUD could not write this report if communities were not able to provide reliable, aggregate data on the clients they serve.

[2] 24 CFR Part 578.57 Homeless Management Information System: http://www.ecfr.gov/cgi24bin/retrieveECFR?gp=&SID=5d030234903ffc25ad85a1fe4656bff7&mc=true&n=pt24.3.578&r=PART&ty=HTML#se24.3.578_165

Section 1: HMIS Governance Structure

HPAC's HMIS governance structure features a tripartite composition of the following roles:

- System Administrator
- Lead Agency
- Daily Operator

Pursuant to HPAC's Governance Charter, Sacramento Steps Forward (SSF) serves as the region's HMIS System Administrator; Yolo Community Care Continuum (YCCC) serves as the region's HMIS Lead Agency; and the County of Yolo serves at the region's HMIS Daily Operator.

HMIS System Administrator

As the HMIS System Administrator, SSF:

Software

- Selects the HMIS software provider
- Serves as primary liaison between the HMIS software provider and the Partner Agencies
- Contracts with the HMIS software provider to administer and maintain central backup server operations including security procedures and daily system backup to prevent the loss of data

Technical

- Issues new user accounts and passwords
- Prompts users to periodically change their passwords for security purposes
- Inactivates user accounts after a specified period of inactivity
- Notifies agencies of HMIS failures and/or system errors immediately upon discovery
- Facilitates the initial software training for all new HMIS users
- Provides training materials, including user manuals with definitions and instructions to each individual who attends the initial training

Privacy and Security

- Maintains all client-identifying information in the strictest of confidence, using the latest available technology
- Monitors access to HMIS in order to detect violations of information security protocols
- Maintains accurate logs of all changes made to the information contained within the database for inspection purposes
- Investigates suspected breaches of confidentiality and suspends HMIS access accordingly
- Develops privacy and security protocols as it pertains to system safety and data integrity

HMIS Lead Agency

As the HMIS Lead Agency, YCCC:

General

- Serves as the primary liaison for any HUD-related requirements including submitting the CoC Consolidated Application and the CoC Planning Grant
- Manages and administers all HMIS-related invoicing and payment processing

HMIS Daily Operator

As the HMIS Daily Operator, the County of Yolo:

General

- Informs HPAC of key HUD and SSF policies related to HMIS
- Facilitates quarterly HPAC Data Subcommittee meetings to discuss system wide challenges
- Attends SSF HMIS meetings including their HMIS End-Users Meetings and their HMIS and Data Committee Meetings
- Shares relevant/important information from SSF HMIS meetings as needed
- Coordinates the collection of data for HUD reports
- Submits reports to HUD as required
- Assists Partner Agencies with HUD or other funding reports and grant applications as needed
- Promotes HMIS usage among all homeless service providers regardless of funding source
- Provides all other reasonably expected activities regarding the day-to-day implementation and operation of HMIS

Technical

- Serves as the primary liaison between the Partner Agencies and SSF
- Ensures that HPAC is compliant with the latest HMIS data standards as prescribed by HUD and SSF
- Programs new projects according to HUD's latest HMIS Data Standards
- Initiates and maintains interagency data sharing options in HMIS
- Provides refresher trainings as needed, including one-on-one trainings
- Resets usernames and passwords as needed
- Merges duplicate records as needed
- Visits agency sites to learn about/resolve issues as needed
- Provides help desk service by responding within 48 hours of an inquiry
- Works with SSF to develop, implement, and maintain written HMIS policies and procedures including a security and privacy plan as well as a data quality plan in accordance with HUD's final rulings
- Identifies potential data quality issues and recommends actions for improvement

HPAC Data Subcommittee

Another component of HPAC's HMIS governance structure is the Data Subcommittee. Serving as an advisory group to the full HPAC body, the Data Subcommittee makes critical recommendations about issues related to HMIS.

The Data Subcommittee's tasks include working with the HMIS System Administrator, HMIS Lead Agency, and HMIS Daily Operator to:

- Annually review this manual and any other HMIS policies and procedures required by HUD and provide recommendations to the full HPAC body for final approval
- Develop and implement a plan for monitoring HMIS to ensure that:
    - HMIS is satisfying the requirements of all regulations and notices issued by HUD
    - The HMIS System Administrator, HMIS Lead Agency, and HMIS Daily Operator are fulfilling the obligations outlined in the HPAC Governance Charter, in the HPAC Policies and Procedures Manual, and in this HPAC HMIS Policies and Procedures Manual
    - Agencies adhere to HPAC's data quality as well as privacy and security standards, which includes reviewing project reports and/or audits and developing technical assistance plans
- Review and approve the final submission of the following counts and reports:
    - Sheltered and Unsheltered Point-In-Time Counts (PIT)
    - Housing Inventory Count (HIC)
    - Annual Homeless Assessment Report (AHAR)
    - Annual HUD System Performance Measures Report

Comprised of at least one representative from each HMIS Partner Agency, the Data Subcommittee meets on a quarterly basis, on the third Wednesday of January, April, July and October from 8:30 to 9:30 a.m. among rotating locations in Davis, West Sacramento, and Woodland. The County of Yolo's Homeless Analyst staffs the Data Subcommittee by scheduling the meetings, creating the agendas, facilitating the discussions, recording the minutes, and sharing recommendations with the full HPAC body.

Section 2: General Operating Policies and Procedures

The following subsections describe several of HPAC's general HMIS operating policies and procedures.

How to Add an Agency

To add an agency to HPAC's HMIS, the agency under consideration must complete the following steps and/or agree to the following stipulations:

1. Contact the HMIS Daily Operator
2. Read the following HPAC documents:
    - HPAC Governance Charter
    - HPAC Policies and Procedures Manual
    - HPAC HMIS Policies and Procedures Manual
3. Complete and submit the following forms to the HMIS Daily Operator:
    - SSF New Project Agency Add Form
    - HPAC HMIS Agency Partner Agreement
    - HPAC Interagency HMIS Data Sharing Agreement
4. Adopt either HPAC's standard Privacy Statement (provided by the Homeless Analyst) or your own agency-specific Privacy Statement that satisfies all of the criteria listed in the 2004 HMIS Data and Technical Standards (see Section 4: HMIS Privacy and Security—Privacy Statement)
5. Post the Privacy Statement, along with the Consumer Notice and List of Participating Agencies (provided by the Homeless Analyst) at your intake desk(s) or comparable location(s)
6. If your agency maintains an agency website, post a link to the Privacy Statement on the homepage of the agency's website
7. Agree to ensure that hard copies of the Privacy Statement, Consumer Notice, and List of Participating Agencies are available upon a client's request
8. Agree to the cost/invoicing process as explained below:
    - As the HMIS Lead Agency, YCCC oversees the cost/invoicing process. As such, YCCC invoices on a quarterly basis during the months of January, April, July, and October. All payments are due to YCCC upon receipt of the invoice. An HMIS Lead Agency cannot fund HMIS utilization on behalf of any other agency.
    - The cost breakdown for each agency is based on:
        - A one-time user activation fee of $175 per user
        - A CoC fee of $5,400 divided equally among the number of Partner Agencies
        - A user fee of $30 per user per month

How to Add a New Project

To add a new project to an already existing agency:

1. Contact the HMIS Daily Operator
2. Read, complete, and submit the following form to the HMIS Daily Operator:
    - SSF New Project Add Form
        - Please note the form does not need to be complete upon submittal. Typically, programming a new project is an iterative process that requires several revisions to ensure accurate tracking of outcomes

How to Add a User

To add a user to an already existing agency:

1. Contact the HMIS Daily Operator
2. Read, complete, and submit the following forms to the HMIS Daily Operator for each new user:
    - SSF HMIS User Account Request Form
    - SSF HMIS User's Agreement
        - Please note this form requires a Human Resources representative or Executive Director to sign the agreement, attesting that the agency conducted a criminal background check on the new user(s)
        - The HMIS System Administrator will deny HMIS access to any potential new users who pleaded no contest or were convicted of any fraud (including identity theft) or stalking related felony crimes punishable by imprisonment of one year or more in any state (see Section 4: HMIS Privacy and Security—Background Check)
        - The HMIS Daily Operator will forward the completed paperwork to SSF by emailing hmis@sacstepsfoward.org and copying the new user(s)
3. Signup for a New End-User Training by visiting https://sac.clarityhs.com/login and completing the online RSVP form
    - As the HMIS System Administrator, SSF facilitates all new user trainings and requires participation in the training prior to receiving access to the local HMIS
    - At the training, the new user(s) will receive his or her username(s) and password(s)
    - SSF typically schedules the trainings on the third Friday of every month

How to Discontinue an Agency

To discontinue an agency:

1. Send a message to the HMIS Daily Operator containing the following information:
    - Reason for discontinuation
    - Official date agency wishes to discontinue use
        - Prior to contacting the HMIS Daily Operator, please ensure that your agency exited all active clients for each project(s). To do so, run a "Program Roster" report and select the "Active" status for each project(s)
2. The HMIS Daily Operator will then share the message with the HMIS Lead Agency
    - Together, the agency, the HMIS Lead Agency, and the HMIS Daily Operator will determine the appropriate final payment amount and agree upon a final date for discontinued use
    - As the cost/invoicing process is on a quarterly schedule, agencies may have to wait until the end of a quarter to discontinue use

How to Discontinue a Project

To discontinue a project:

1. Send a message to the HMIS Daily Operator containing the following information:
    - Name of project to be discontinued
    - Reason for discontinuation
    - Official date project ended
        - Prior to contacting the HMIS Daily Operator, please ensure that your agency exited all active clients for each project. To do so, run a "Program Roster" report and select the "Active" status

How to Discontinue a User

To discontinue a user:

1. Send a message to the HMIS Daily Operator containing the following information:
    - Name of user to be discontinued
    - Reason for discontinuation
    - If applicable, date of separation to ensure activation is not terminated preemptively

How to Request Technical Assistance

To request technical assistance:

1. Send a message to the HMIS Daily Operator containing the following information:
    - Detailed summary of the issue
    - If applicable, client unique ID number(s)
    - Call back number
    - Please indicate if the issue is urgent e.g. need to submit a report by a particular deadline
        - The HMIS Daily Operator will respond to your request within 48 hours of receipt unless it is a county-recognized holiday and/or the agency receives an out of office reply

How to Request a Merging of Two Records

To request a merging of two records:

1. Send a message to the HMIS Daily Operator containing the following information:
    - Name
    - Client unique ID numbers of the records to be merged
        - Please indicate which record the user thinks should be the surviving record
    - Please indicate if the issue is urgent e.g. need to submit a report by a particular deadline
        - The HMIS Daily Operator will respond to your request within 48 hours of receipt unless it is a county-recognized holiday and/or the agency receives an out of office reply

How to Request a Password Reset

To request a password reset:

2. Send a message to the HMIS Daily Operator containing the following information:
    - Name
    - Please indicate if the issue is urgent e.g. need to submit a report by a particular deadline
        - The HMIS Daily Operator will respond to your request within 48 hours of receipt unless it is a county-recognized holiday and/or the agency receives an out of office reply
        - The HMIS Daily Operator will respond with a username and a temporary password. Upon logging in, the system will prompt the user to enter a new password

How to Submit a Data Request

To submit a data request:

1. Send a message to the HMIS Daily Operator containing the following information:
    - Detailed summary of data request including:
        - Purpose of the data request
        - Authority who approved this request
        - Requested report period
        - Preferred format for the data file
        - Indicate if this is a system wide report, if not, what project types should be included e.g. only HUD-funded projects

    - Indicate what data elements need to be included
    - Indicate if you would like unduplicated data or all records collected
    - Due date
- Call back number
- Please indicate if the issue is urgent e.g. need to submit a report by a particular deadline
    - The HMIS Daily Operator will respond to your request within 48 hours of receipt unless it is a county-recognized holiday and/or the agency receives an out of office reply

Section 3: HMIS Data Quality Plan

This section describes HPAC's HMIS Data Quality Plan. Developed by the HPAC Data Subcommittee in coordination with the HMIS System Administrator, HMIS Lead Agency, and HMIS Daily Operator, the Plan represents a system-level document that enhances HPAC's ability to achieve statistically valid and reliable data. As such, the Plan:

- Establishes specific data quality benchmarks for timeliness, completeness, bed/unit utilization, bed coverage rates, and service-volume coverage rates
- Describes the procedures for implementing the plan and monitoring progress toward meeting the benchmarks

As stated at the beginning of this manual, HPAC will review, revise, and re-ratify its HMIS Data Quality Plan every October upon a majority vote of all voting members present during the scheduled meeting. Prior to HPAC's vote, the Data Subcommittee will recommend updates to the full HPAC body according to HUD's latest HMIS Data Standards and locally developed performance plans.

HMIS Data Standards

Published in 2014, HUD's HMIS Data Standards serve as the basis for HPAC's Data Quality Plan. Since HUD is responsible for setting forth guidelines regarding HMIS usage, the Standards outline the minimum participation and reporting requirements.

The Standards include three primary components: (1) Universal Data Elements, (2) Program-Specific Data Elements, and (3) Project Descriptor Data Elements.

Universal Data Elements

The Universal Data Elements establish the baseline collection requirements for all agencies entering data into HMIS. In this way, the Universal Data Elements provide the foundation for producing unduplicated estimates of the number of homeless persons receiving services, basic demographic information, and patterns of use such as the length of project stays, exits to permanent housing, chronicity, and the number of homeless episodes over time.

The required Universal Data Elements include:

- 3.1 Name
- 3.2 Social Security Number
- 3.3 Date of Birth
- 3.4 Race
- 3.5 Ethnicity
- 3.6 Gender
- 3.7 Veteran Status
- 3.8 Disabling Condition
- 3.9 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 Emergency Shelter or Safe Haven

Program-Specific Data Elements

Program-Specific Data Elements differ from Universal Data Elements in that no one project must collect every single element in this subsection. Which data elements are required is dictated by the reporting requirements set forth by the project funder.

Many of these data elements represent transactions or information that may change over time. Most agencies capture Program-Specific Data Elements at project entry and exit, but a few must be captured at project entry, exit, and on an annual basis.

The required Program-Specific Data Elements include:

- 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 Condition
- 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 contain basic information about projects participating in a region's HMIS and help ensure HMIS is the central repository of information about homelessness. The Project Descriptor Data Elements very much represent the building blocks of HMIS. They enable the system to:

- Associate client-level records with the various projects that a client will enroll in across a service area
- Clearly define the type of project the client is associated with the entire time he or she received housing and/or services
- Identify which federal partner programs are providing funding to the project
- Track bed and unit inventory and other information, by project, which is relevant for:
    - Sheltered and Unsheltered Point-In-Time Counts (PIT)
    - Housing Inventory Count (HIC)
    - Annual Homeless Assessment Report (AHAR)
    - Data Quality Monitoring Reports
    - System Performance Measures Report

The HMIS Daily Operator and/or HMIS System Administrator, not the agency or user, generally enters and manages Project Descriptor Data Elements. As such, the HMIS Daily Operator and/or HMIS System Administrator enter this information upon project setup, but will conduct an annual verification of the information and update the information as needed (see Other Important Data Quality Practices—Annual Verifications).

The required Project Descriptor Data Elements include:

- 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

Goals and Benchmarks

Timeliness

Timeliness refers to how much time elapses from when a user collects data from a client to when a user inputs the data into HMIS. Thus, the system compares the difference between the project entry/exit date specified for the client and the date the user enters the information into HMIS. For example, if a user inputted a project entry date of April 4 (the date of the client's intake assessment), but the current date is April 9, then there would be a five (5) day lag time in entering the data.

There are numerous reasons why timely data entry is important. First, it minimizes the likelihood of human error that can occur when too much time has passed between the data collection and the data entry. Timely data entry also ensures that the data is readily accessible, whether for monitoring purposes or for meeting funding requirements. Lastly, timeliness is a critical component of coordinated entry as it relies on up-to-date bed/unit availability in order to make referrals.

While HPAC highly encourages live data entry, HPAC acknowledges that there are circumstances when live data entry may not be possible. As such, HPAC set the following goal and corresponding benchmarks for each project type:

Goal	At least 95% of all data entry should fall within the specified timeliness benchmarks

Project Type	**Benchmark**
Emergency Shelter	Agency to enter all Universal Data Elements and Project-Specific Data Elements within three (3) days of intake and/or exit
Transitional Housing	Agency to enter all Universal Data Elements and Project-Specific Data Elements within three (3) days of intake and/or exit
Permanent Housing	Agency to enter all Universal Data Elements and Project-Specific Data Elements within three (3) days of intake and/or exit

Permanent Supportive Housing	Agency to enter all Universal Data Elements and Project-Specific Data Elements within three (3) days of intake and/or exit
Prevention and Rapid Re-Housing	Agency to enter all Universal Data Elements and Project-Specific Data Elements within three (3) days of intake and/or exit
Street Outreach	Agency to enter all Universal Data Elements and Project-Specific Data Elements within three (3) days of intake and/or exit
Supportive Services Only	Agency to enter all Universal Data Elements and Project-Specific Data Elements within three (3) days of intake and/or exit

It is important to note that users cannot back enter or edit data to fix timeliness. Rather users can only strive to improve data timeliness for future entries.

Completeness

Completeness refers to the number of "Missing/Data Not Collected" and "Client Doesn't Know/Client Refused" responses collected for both the required Universal Data Elements and Project-Specific Data Elements.

Complete data is key to assisting clients end their homelessness. Not only does incomplete data hinder an agency's ability to provide comprehensive care, but incomplete data also negatively affects HPAC's ability to identify service deficiencies and devise effective strategies for improvement. In addition, HMIS data quality is a component of most federal funding applications and low HMIS data quality scores may affect renewal funding as well as future funding requests. Given its importance, HPAC set the following goal and corresponding benchmarks for each project type and data element.

Goal	At least 95% of all data entry should fall within the specified completeness benchmarks

Universal Data Element	**Benchmark**					
	Emergency Shelter and Non-HUD Supportive Services Only		HUD Supportive Services Only, Transitional Housing, Permanent Housing, Permanent Supportive Housing, Prevention, and Rapid Re-Housing		Street Outreach	
	Missing/Data Not Collected	Client Doesn't Know/Client Refused	Missing/Data Not Collected	Client Doesn't Know/Client Refused	Missing/Data Not Collected	Client Doesn't Know/Client Refused
3.1 Name	0%	0%	0%	0%	0%	0%
3.2 Social Security Number	0%	0%	0%	5%	0%	5%
3.3 Date of Birth	0%	0%	0%	5%	0%	5%

3.4 Race	0%	0%	0%	5%	0%	5%
3.5 Ethnicity	0%	0%	0%	5%	0%	5%
3.6 Gender	0%	0%	0%	0%	0%	0%
3.7 Veteran Status	0%	0%	0%	5%	0%	5%
3.8 Disabling Condition	0%	0%	0%	5%	0%	5%
3.9 Residence Prior to Project Entry	0%	0%	0%	0%	0%	0%
3.10 Project Entry Date	0%	0%	0%	0%	0%	0%
3.11 Project Exit Date	0%	0%	0%	0%	0%	0%
3.12 Destination	5%	5%	5%	5%	15%	5%
3.15 Relationship to Head of Household	0%	0%	0%	0%	0%	0%
3.16 Client Location	0%	0%	0%	0%	0%	0%
3.17 Length of Time on Street or in an Emergency Shelter	0%	0%	0%	0%	0%	0%

Program-Specific Data Element	**Benchmark**					
	Emergency Shelter and Non-HUD Supportive Services Only		HUD Supportive Services Only, Transitional Housing, Permanent Housing, Permanent Supportive Housing, Prevention, and Rapid Re-Housing		Street Outreach	
	Missing/Data Not Collected	Client Doesn't Know/Client Refused	Missing/Data Not Collected	Client Doesn't Know/Client Refused	Missing/Data Not Collected	Client Doesn't Know/Client Refused
4.1 Housing Status	0%	0%	0%	0%	0%	0%
4.2 Income and Sources	0%	0%	0%	0%	0%	0%
4.3 Non-Cash Benefits	0%	0%	0%	0%	0%	0%
4.4 Health Insurance	0%	0%	0%	0%	0%	0%
4.5 Physical Disability	0%	0%	0%	0%	0%	0%
4.6 Developmental	0%	0%	0%	0%	0%	0%

Disability						
4.7 Chronic Health Condition	0%	0%	0%	0%	0%	0%
4.8 HIV/AIDS	0%	0%	0%	0%	0%	0%
4.9 Mental Health Problem	0%	0%	0%	0%	0%	0%
4.10 Substance Use	0%	0%	0%	0%	0%	0%
4.11 Domestic Violence	0%	0%	0%	0%	0%	0%
4.12 Contact	N/A	N/A	N/A	N/A	0%	0%
4.26 Employed	0%	0%	5%	5%	5%	5%

Unlike timeliness, users can fix completeness by back entering or editing data. Thus, HPAC highly encourages users to routinely monitor completeness and update any records that exceed the benchmarks listed above. In some circumstances, this may require staff to re-review paper intake forms or even re-contact the client.

Bed/Unit Utilization Rates

Bed/unit utilization rates compare the number of occupied beds/units to the project's entire bed/unit inventory. Thus, the rates are equal to the number of occupied beds/units divided by the number of total beds/units available.

A core feature of HMIS is its ability to record the number of nights a client stays at a residential housing project. When an agency admits a client into a residential project, HMIS assigns the client a housing service. Named "Housed with—name of the project or funding source," the housing service remains active until the agency exits the client from the project.

Thus, a project's bed/unit utilization rate is an excellent barometer of data quality. A low utilization rate could reflect low occupancy, but it could also indicate that an agency is not entering data into HMIS for every client served. A high utilization rate could reflect that the project is over capacity, but it could also indicate that an agency has not properly exited clients from the project in HMIS. More specifically, bed utilization can legitimately exceed 105% for two main reasons. First, the project offers overflow beds—e.g. cots or mattresses—sporadically throughout the year to accommodate high-demand nights, which results in a larger count of persons than the average number of year-round beds reported on the Housing Inventory Count. Second, the project serves a family with more children than the beds reported as part of the year's Housing Inventory Count. A third reason, related to a data quality issue, is that the project operator is not entering accurate project entry or exit dates, which causes an overlap in stays.

Using HUD's Annual Homeless Assessment Report (AHAR) guidelines, HPAC set the following goal and benchmarks for all residential housing projects.

Goal	100% of all data entry should fall within the specified utilization benchmarks

Project Type	Benchmark
Emergency Shelter	65 to 105%
Transitional Housing	65 to 105%
Permanent Supportive Housing	65 to 105%

Similar to completeness, users can fix bed/unit utilization rates by back entering or editing data. HPAC highly encourages users to routinely monitor bed/unit utilization rates to ensure true occupancy rates are accurately reflected within HMIS. In addition, HPAC recognizes that new projects may require time to reach their projected occupancy numbers and will not expect them to meet the utilization benchmark during the first six months of operation.

Bed Coverage Rates

Bed coverage rates compare the total number of beds in HMIS divided by the total bed inventory. The bed coverage rate should account for all HPAC beds in the community, including both HUD and non-HUD funded beds.

This is an important rate to calculate to ensure that HPAC meets HUD's minimum threshold of at least 50% to be eligible for the Annual Homeless Assessment Report (AHAR). Without meeting the 50% threshold, HUD is unable to project estimates for non-HMIS projects with reasonable statistical confidence.

Despite the 50% threshold, HPAC will strive to achieve an even higher standard of 85% as prescribed in HUD's CoC application. The HMIS Daily Operator will calculate these rates annually for the CoC application as well as in preparation for the AHAR.

Goal	At least 85% bed coverage rate for all project types

Service-Volume Coverage Rates

Service-volume coverage rates compare the number of persons served annually by any given project that participates in HMIS divided by the number of persons served annually by all HPAC projects in the community.

This is an important rate to calculate to ensure that HPAC meets HUD's minimum threshold of at least 50% to be eligible for the Annual Homeless Assessment Report (AHAR). Without meeting the 50% threshold, HUD is unable to project estimates for non-HMIS projects with reasonable statistical confidence.

Despite the 50% threshold, HPAC will strive to achieve an even higher standard of 85% as prescribed in HUD's CoC application. The HMIS Daily Operator will calculate these rates annually for the CoC application as well as in preparation for the AHAR.

Goal	At least 85% service-volume coverage rate for all project types

Other Important Data Quality Practices

HPAC will implement two other important practices as part of its HMIS Data Quality Plan. The practices involve an annual verification of Project Descriptor Data Elements and residential housing projects as well as establishing local standards regarding accuracy.

Annual Verifications

Every year prior to the Annual Homeless Assessment Report (AHAR), the HMIS Daily Operator will request agencies to verify their Project Descriptor Data Elements (see Section 3: HMIS Data Quality Plan—Project Descriptor Data Elements) as well as their inventory of residential housing projects.

This practice will ensure that bed/unit utilization rates are accurate and therefore AHAR reporting is accurate. Collecting such information will also be helpful for the numerous annual reports required by HUD including the Point-In-Time Count (PIT), the Housing Inventory Count (HIC), and the System Performance Measure Report.

Accuracy

HMIS data needs to accurately represent the clients served and the services provided. The best way to measure accuracy is to compare the HMIS data with primary sources such as a social security card, birth certificate, or driver's license. To ensure the most up-to-date and complete data, HPAC recommends internal data quality monitoring on a monthly basis.

Another important aspect of maintaining data integrity is collecting and entering data in a common and consistent manner across all projects. To that end, the HPAC Data Subcommittee will regularly review best practices and discuss common problems.

Some important things to note regarding accuracy include:

- All Universal Data Elements and Program Specific Data Elements must be obtained from each adult and unaccompanied youth who apply for services
- 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. HUD considers these valid responses if the client does not know or the client refuses to respond to the question. It is not the intention of HUD, or any other funders who require HMIS usage, to have agencies deny clients 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.
- Agencies should not use the "Client Doesn't Know" or "Client Refused" responses to indicate that the case manager or data entry staff member does not know the client's response
- Since HPAC's HMIS requires a response to all data fields before saving a record, the agency should use the "Data not collected" response to indicate missing data

Monitoring

The purpose of monitoring is to ensure that agencies are meeting or are as close as possible to meeting the agreed-upon data quality goals and benchmarks. Monitoring will also help agencies quickly identify and ideally resolve data quality issues.

The following subsections review the roles and responsibilities of each entity in the monitoring process and establish a monitoring schedule.

Monitoring Roles and Responsibilities

HMIS System Administrator

The HMIS System Administrator is responsible for the ongoing maintenance of the existing data quality report, which includes working with the HMIS software vendor to update the report to reflect HUD's latest HMIS Data Standards. The HMIS System Administrator is also responsible for providing initial training to new users, teaching best practices for HMIS data entry.

HMIS Daily Operator

The HMIS Daily Operator is responsible for providing technical assistance to Partner Agencies that need help addressing data quality issues. The HMIS Daily Operator is also responsible for providing ongoing training beyond the initial training provided by the HMIS System Administrator.

HPAC Data Subcommittee

The HPAC Data Subcommittee is responsible for reviewing each project's data quality on a quarterly basis. The Data Subcommittee will work to identify issues that do not comply with the agreed-upon goals and benchmarks. Based from the Data Subcommittee's assessment, the HMIS Daily Operator will offer individualized support and develop specialized trainings as necessary.

HMIS Partner Agency

The HMIS Partner Agency is responsible for pulling data quality reports and correcting data entry errors for each project within HMIS.

Monitoring Schedule

As stated above, the HPAC Data Subcommittee will monitor the data quality of all active projects within HMIS on a quarterly basis. The Data Subcommittee meets on a quarterly basis, on the third Wednesday of January, April, July and October from 8:30 to 9:30 a.m. among rotating locations among Davis, West Sacramento, and Woodland. The County of Yolo's Homeless Analyst, who staffs the Data Subcommittee, will prepare data quality reports prior to the quarterly meetings.

Section 4: HMIS Privacy and Security Plan

This section describes HPAC's HMIS Privacy and Security Plan. Developed by the HPAC Data Subcommittee in coordination with the HMIS System Administrator, HMIS Lead Agency, and HMIS Daily Operator, the Plan represents a system-level document that enhances HPAC's ability to protect the privacy and security of the information collected and stored in HMIS. As such, the Plan:

- Addresses federal regulations related to HMIS privacy and security
- Delineates specific roles and responsibilities for the HMIS System Administrator, the HMIS Daily Operator, the HMIS Partner Agency, and the HMIS End User
- Establishes system security safeguards
- Describes the procedures for implementing the plan and monitoring for compliance

As stated at the beginning of this manual, HPAC will review, revise, and re-ratify the HMIS Privacy and Security Plan every October upon a majority vote of all voting members present during the scheduled meeting. Prior to HPAC's vote, the Data Subcommittee will recommend updates to the full HPAC body according to HUD's latest HMIS standards.

It is important to note that the Plan complies with HUD's 2004 HMIS Data and Technical Standards Final Notice[3] as well as state and local laws regulating the confidentiality of personal information. Yet, at the time of writing this Plan, HUD has not yet released a final notice regarding HMIS security. Given this, the Plan contains preliminary security safeguards; however, HPAC anticipates updating the safeguards upon receiving final guidance from HUD.

It is also important to note that HPAC wrote the Plan in support of an open HMIS system, where data sharing occurs amongst agencies who opted to be part of the HPAC Data Sharing Agreement. While HPAC recognizes that individual agencies serve clients, HPAC equally recognizes that the region's entire homeless services system serves clients.

HMIS Data and Technical Standards

The core tenets of HPAC's Privacy and Security Plan are the requirements specified in the 2004 HMIS Data and Technical Standards Final Notice[4]. The following subsections explain each requirement and HPAC's standards for compliance.

Privacy Statement

The Privacy Statement describes how an agency collects, uses, and discloses client information. The Privacy Statement must also describe how a client can access his or her information. HPAC requires that each agency either adopt HPAC's standard Privacy Statement or adopt their own agency-specific Privacy Statement, which meets all of the minimum requirements set forth in HUD's 2004 HMIS Data and Technical Standards Final Notice[5] (see Additional Information about the Privacy Statement).

---

[3] 2004 HMIS Data and Technical Standards Final Notice:
https://www.hudexchange.info/resources/documents/2004HUDDataandTechnicalStandards.pdf

[4] 2004 HMIS Data and Technical Standards Final Notice:
https://www.hudexchange.info/resources/documents/2004HUDDataandTechnicalStandards.pdf

[5] 2004 HMIS Data and Technical Standards Final Notice:
https://www.hudexchange.info/resources/documents/2004HUDDataandTechnicalStandards.pdf

In addition to having a Privacy Statement, HPAC requires that HMIS Partner Agencies, who have a website, post a link to the Privacy Statement online. HPAC also requires that Partner Agencies post the Privacy Statement at each intake desk(s) or a comparable location(s). Lastly, HPAC requires that all staff have access to hard copies of the Privacy Statement when out in the field.

Additional Information about the Privacy Statement

As stated above, every HMIS Partner Agency must have a Privacy Statement that describes how and when the agency will use and disclose a client's Protected Personal Information (PPI). PPI includes name, Social Security Number (SSN), date of birth, zip code, project entry and/or exit date.

Partner Agencies may be required to collect a client's PPI by law or by funders. Partner Agencies also collect PPI to monitor project operations, to better understand the needs of persons experiencing homelessness, and to improve services for persons experiencing homelessness. HPAC only permits agencies to collect PPI with a client's written consent.

Partner Agencies may use and disclose 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.

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 the client's 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 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 an agency denies a client's request, the client should receive a written explanation for the denial. The client has the right to appeal the denial by following the established HPAC Partner Agency Agreement grievance procedure. Regardless of the outcome of the appeal, the client will have the right to add to his or her project records a concise statement of disagreement. The agency must 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.

Partner Agencies can amend their Privacy Statements 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. The agency must make available a record of all amendments to the Privacy Statement upon a client's request.

As stated previously, a Privacy Statement must reflect, at a minimum, the baseline requirements outlined within HUD's 2004 HMIS Data and Technical Standards Final Notice. In any instance where an agency's Privacy Statement is not consistent with HUD standards, HUD standards will take precedence.

Consumer Notice

The Consumer Notice explains the reason for asking for personal information and notifies the client of the Privacy Statement. HPAC requires that agencies either adopt HPAC's standard Consumer Notice or adopt their own Consumer Notice, which meets all of the minimum requirements set forth in HUD's 2004 HMIS Data and Technical Standards Final Notice[6].

In addition to having a Consumer Notice, HPAC requires that participating HMIS agencies post the Consumer Notice at each intake desk(s) or a comparable location(s). Lastly, HPAC requires that all staff have access to hard copies of the Consumer Notice when out in the field.

List of Participating Agencies

The List of Participating Agencies names all current HMIS using providers, which allows clients to see which organizations have access to their information. The HMIS Daily Operator will provide updated lists when necessary.

HPAC requires that participating HMIS agencies post the List of Participating Agencies at each intake desk(s) or a comparable location(s). Lastly, HPAC requires that all staff have access to hard copies of the List of Participating Agencies when out in the field.

Informed Consent and Release of Information Authorization

The Informed Consent and Release of Information Authorization must be signed by all adult clients and unaccompanied youth. This gives the client the opportunity to refuse the sharing of his or her information to

[6] 2004 HMIS Data and Technical Standards Final Notice:
https://www.hudexchange.info/resources/documents/2004HUDDataandTechnicalStandards.pdf

other agencies within the system. HPAC requires client signatures prior to inputting their information in HMIS. HPAC also requires agencies to update Informed Consent and Release of Information Authorization forms every five years.

Privacy and Security Safeguards

This section describes the various safeguards in place to protect the privacy and security of the information collected and stored in HMIS. It is important to note that all agency executive directors or program managers are responsible for understanding these safeguards and effectively communicating these safeguards to individuals responsible for privacy and security at their agency.

It is also important to underscore that all HMIS Partner Agencies must apply the safeguards explained below. Additionally, HPAC expects that agencies apply the safeguards to all networked devices. This includes, but is not limited to, networks, desktops, laptops, mobile devices, tablets, mainframes, and servers.

Physical Safeguards

In order to protect client privacy, agencies must implement the following physical safeguards. For the purposes of this section, HPAC defines authorized users as HMIS End Users who have received the New End User Training and have signed New End User Agreements on file with the HMIS System Administrator.

Computer Location

A computer used as an HMIS workstation must be in a secure location where only authorized staff members have access. The workstation must not be accessible to clients, the public, or volunteers. HPAC also requires that any computer accessing HMIS enable a password protected automatic screensaver.

Printer Location

HPAC requires that users send HMIS documents to a printer located in a secure location where only authorized staff members have access.

Monitor

Non-authorized users should not be able to see an HMIS workstation screen. HPAC advises users to turn monitors away from the public view and utilize visibility filters to protect client privacy.

Mobile Device

A mobile device and/or tablet used to access and enter information into HMIS must use a password or other user authentication on the lock screen to prevent an unauthorized person from accessing it. In addition, the device and/or tablet should be set to automatically lock after a set period of inactivity. HPAC also recommends that users download a remote wipe and/or remote disable option onto the device.

Technical Safeguards

Workstation Security

To promote the security of HMIS and the confidentiality of the data contained therein, HPAC will only allow access to HMIS through approved workstations. To ensure compliance, the HMIS System Administrator 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). Users will be required to submit the IP Address of their workstation to the HMIS System Administrator to be registered into the system and will notify the System Administrator should this number need to be changed.

Establishing HMIS User IDs and Access Levels

HPAC prohibits the sharing of usernames and passwords by or among more than one end user. To that end, the HMIS System Administrator will assign the most restrictive access level, while still allowing the end user to efficiently and effectively perform his or her duties.

User Authentication

- Usernames are individual and passwords are confidential. No individual should ever use or allow use of a username that is not assigned to that individual and passwords should never be shared or communicated in any format
- The system requires users to change temporary passwords upon first use. Passwords must be a minimum of six (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 ninety (90) 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 username until the HMIS Daily Operator resets the password
- End 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 at least 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 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 must notify the HMIS System Administrator to deactivate the user's license while the Partner Agency Security Office conducts an internal agency investigation
- Any user found to have misappropriated client data (identity theft, releasing personal client data to any unauthorized party) will have his or her HMIS privileges revoked
- HPAC is empowered to permanently revoke a Partner Agency's access to HMIS for substantiated noncompliance with the provisions of this Plan 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

- HPAC requires that each HMIS Partner Agency develop and implement procedures for managing new, retired, and compromised local system account credentials
- HPAC requires that each HMIS Partner Agency 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

Disaster Recovery Policy

The HMIS System Administrator is responsible for facilitating recovery from a disaster with support from the HMIS software vendor as needed. As such, the System Administrator must:

- Be aware of and be trained to complete any tasks or procedures for which they are responsible in the event of a disaster
- Have a plan for restoring local computing capabilities and internet connectivity for the HMIS System Administrator's facilities
- Maintain a readily accessible list of account numbers and contact information for its internet service provider, support contracts, and equipment warranties
- Maintain a list of the computer and network equipment required to restore minimal access to HMIS and to continue providing services to HMIS Partner Agencies
- Maintain documentation of the configuration settings required to restore local user accounts and internet access

Workforce Security Policy

HMIS Access to Active Clients

HPAC has an open 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, HPAC 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 HPAC or Sacramento CoC HMIS.

- The HMIS System Administrator will search the individual in HMIS before issuing HMIS access
- The HMIS System Administrator will deny access to individuals who are active in HMIS

Background Check Policy

HMIS End User Background Check Requirements

HPAC recognizes the sensitivity of the data in HMIS, and therefore requires that the individuals responsible for managing HMIS be subject to a criminal background check.

The HMIS System Administrator will deny access to HMIS if a staff member's background check reveals a history of any of the following crimes:

- 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 an individual offers money, goods, services, information or anything else of value 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

In order to comply with this safeguard, HMIS Partner Agencies must have a policy regarding conducting background checks and hiring individuals with criminal justice histories. The policy should require that all end users have a background check prior to requesting HMIS access.

Monitoring

HPAC will monitor adherence to the Plan using the following structure and measures.

Roles and Responsibilities

HMIS System Administrator

As the HMIS System Administrator, SSF:

- Prevents degradation of the system resulting from viruses, intrusion, or other factors within the System Administrator's control
- Prevents inadvertent release of confidential client-specific information through physical or electronics access to system servers

HMIS Daily Operator

As the HMIS Daily Operator, the County of Yolo:

- Provides technical assistance to agencies and users who need assistance complying with HPAC's Privacy and Security Plan

HPAC Data Subcommittee

As an advisory group to the full HPAC body, the Data Subcommittee:

- Makes annual recommendations to the full HPAC body regarding revisions to the Plan

- Monitors agencies and users to ensure adherence to the roles and responsibilities delineated within HPAC's Privacy and Security Plan
- Develops technical assistance, action and/or compliance plans for agencies that the Data Subcommittee finds to be in violation of HPAC's Privacy and Security Plan

HMIS Partner Agency

The HMIS Partner Agency:

- Prevents degradation of the HMIS resulting from viruses, intrusion, or other factors within the agency's control and prevents the inadvertent release of confidential client-specific information through physical, electronic or visual access to user workstations
- Ensures the agency meets the privacy and security requirements detailed in the HUD HMIS Data and Technical Standards
- Adopts and upholds a Privacy Statement, which meets or exceeds all minimum standards including substance use providers covered by 24 CFR Part 2, HIPPA covered agencies
    - Modifications to HPAC's standard Privacy Statement must be approved by the HPAC Data Subcommittee
- Ensures 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
- Makes reasonable accommodations for persons with disabilities, language barriers, or education barriers
- Ensures that anyone working with clients covered by the Privacy Statement can meet the user responsibilities
- Designates at least one Security Officer that has been trained to technologically uphold the adopted Privacy Statement

HMIS End User

HPAC defines an HMIS end user as a person that has direct interaction with a client and/or his or her data including but not limited to PPI. Therefore, an end user:

- Reads and understands his or her agency's Privacy Statement
- Has the ability to explain his or her agency's Privacy Statement to clients
- Adheres to his or her agency's Privacy Statement
- Knows where to refer a client if he or she cannot answer a question
- Completes an Informed Consent and Release of Information Authorization with a client prior to collecting and inputting HMIS data
- Presents his or her agency's Privacy Statement to a client before collecting any information
- Upholds a client's privacy in HMIS

Security Officers

To further assist with the monitoring, all HMIS Partner Agencies must designate a Partner Agency Security Officer to ensure adherence to HPAC's Privacy and Security Plan.

Lead Security Officer

- May be the HMIS System Administrator or another employee, volunteer or contractor designated by SSF who has completed HMIS Privacy and Security training 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

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 semiannually for all agency HMIS workstations
    - Prior to issuing a User ID to a new HMIS End User
    - 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 semiannual 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 the duties assigned to the Partner Agency Security Officer.

- 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

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 (i.e. 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 HPAC 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 fifteen (15) days

- Any Checklist that includes one 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 one project site, at least one 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 HPAC 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 fifteen (15) days
- Any Checklist that includes one 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

Reporting Security Incidents

While HPAC intends for the monitoring to prevent, to the greatest degree possible, any security incidents, should a security incident occur, an agency should comply with the following reporting procedures:

- Any user who becomes aware of or suspects a compromise in HMIS security and/or client privacy must immediately report the concern to their agency's Security Officer.
- In the event of a suspected security or privacy concern, the agency Security Officer should complete an internal investigation
- If the suspected security or privacy concern resulted from a user's suspected or demonstrated noncompliance with the HMIS End User Agreement, the Security Officer should have the HMIS System Administrator deactivate the user's account until the internal investigation has been completed
- Following the internal investigation, the Security Officer should 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 a user with a signed HMIS End User Agreement, the Lead Security Officer reserves the right to permanently deactivate the user account for the 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 user or agency must implement the action plan as soon as possible, and the total term of the plan must not exceed thirty (30) days

- If the user or agency is not able to meet the terms of the action plan within the time allotted, the HMIS System Administrator, in consultation with the full HPAC body, may elect to terminate the agency's access to HMIS
- The agency may appeal to HPAC 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 the HPAC's Privacy and Security Plan, this manual, or the Privacy Statement, the 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 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 System Administrator will notify HPAC of any substantiated release of PPI in noncompliance with the provisions of HPAC's Privacy and Security Plan, this manual, or the Privacy Statement
- The HMIS System Administrator will maintain a record of all substantiated releases of PPI in noncompliance with the provisions of HPAC's Privacy and Security Plan, this manual, or the Privacy Statement for 7 years
- HPAC reserves the right to permanently revoke an agency's access to HMIS for substantiated noncompliance with the provisions of HPAC's Privacy and Security Plan, this manual, or the Privacy Statement that resulted in a release of PPI