2022

HMIS Policies & Procedures

MONTEREY & SAN BENITO COUNTIES

PREPARED BY: THE COALITION OF HOMELESS SERVICES PROVIDERS

Contents

HMIS Governance Policies and Procedures Overview

This document provides the framework for the ongoing operations of the Monterey and San Benito counties' Homeless Management Information System (HMIS) Project. The Project Overview provides the main objectives, direction, and benefits of the Monterey/San Benito counties' HMIS Project. Governing principles establish the values that are the basis for all policy statements and subsequent decisions.

Operating procedures will provide specific policies and steps necessary to control the operational environment and enforce compliance in the areas of:

- Project Participation
- User Authorization
- Collection of Client Data
- Release of Client Data
- Server Security and Availability
- Workstation Security
- Training
- Technical Support

Other obligations and agreements will discuss the external relationships required to continue this project. Form control provides information on obtaining forms, filing, and record keeping.

Major Updates/Changes to 2022 HMIS Policies and Procedures

- HMIS Licenses cost **$445.00 per license/per year**. This fee is from our vendor, WellSky, and can change at their discretion. Once paid, your agency will own the license for the year and can transfer it to users as needed. If additional licenses are required after, agencies will be charged a prorated rate, and the license will expire annually at the end of **August**.
- **From August 2022 to August 2023 CHSP will subsidize each license by 50%**, as long as funding is available.
- Starting in August 2022 each agency will be billed **$222.50 per license.** CHSP will continue to search for funding to cover license fees.
- CHSP reserves the right to pull licenses that have not been used in over 90 days if funding is limited (See Rescinding User Access)

Introduction

What is HMIS?

A Homeless Management Information System (HMIS) is a local information technology system used to collect client-level data and data on the provision of housing and services to homeless individuals and families, and persons at risk of homelessness. Each Continuum of Care is responsible for selecting an HMIS software solution that complies with HUD's data collection, management, and reporting standards.

The US Department of Housing and Urban Development (HUD) and other planners and policymakers use aggregate HMIS data to better inform homeless policy and decision-making at the federal, state, and local levels. HMIS enables HUD to collect national-level data on the extent and nature of homelessness over time. Specifically, an HMIS can be used to produce an unduplicated count of homeless persons, understand service use patterns, and measure the effectiveness of homeless programs. Data on people experiencing homelessness is collected and maintained at the local level. HMIS implementations can encompass geographic areas ranging from a single county to an entire state.

The HEARTH Act, enacted into law on May 20, 2009, requires that all communities have an HMIS with the capacity to collect unduplicated counts of individuals and families experiencing homelessness. Through their HMIS, a community should be able to collect information from projects serving homeless families and individuals to use as part of their needs analyses and to establish funding priorities. The Act also codifies into law specific data collection requirements integral to HMIS. With the enactment of the HEARTH Act, HMIS participation became a statutory requirement for recipients and sub-recipients of the CoC Program, Emergency Solutions Grant (ESG), SSVF, PATH, RHYMIS, and other funds.

An HMIS can be used to:

- Produce an unduplicated count of persons experiencing homelessness for each CoC
- Describe the extent and nature of homelessness locally, regionally, and nationally
- Identify patterns of service use
- Measure program effectiveness

Project Overview

The long-term vision of HMIS is to enhance Partner Agencies' collaboration, service delivery, and data collection capabilities. Accurate information will put the collaborative in a better position to request funding from various sources and help better plan for future needs. The Monterey and San Benito Counties' HMIS aims to be an integrated network of homeless and other services providers that use a central database to collect, track, and report uniform information on client needs and services. This system will meet federal requirements and enhance service planning and delivery. The fundamental goal of the Monterey/San Benito Counties' HMIS Project is to document the demographics of homelessness in Monterey and San Benito Counties according to the HUD HMIS standards. The project's

goal is to identify patterns in the utilization of assistance and document the effectiveness of the services for the client. This will be accomplished through data analysis gathered from actual experiences of homeless persons, the service providers who assist them in shelters, and other homeless assistance programs throughout the counties. CHSP will use data collected via intake interviews and program participants to complete HUD annual progress reports. CHSP may also analyze this data to provide unduplicated counts and anonymous data to policymakers, service providers, advocates, and consumer representatives.

The project utilizes a web-enabled application on a central server to facilitate data collection by homeless service organizations across the two counties. Access to the central server is limited to agencies formally participating in the project, including only authorized staff members that have met the necessary training and security requirements.

The Monterey/San Benito Counties' HMIS Project is staffed and advised by the Coalition of Homeless Services Providers (CHSP). CHSP's Executive Officer is the authorizing agent for all agreements between Partner Agencies and CHSP. In addition, CHSP staff are responsible for coordination, training, and user access. CHSP staff will also provide technical assistance to system users throughout the two counties.

The Monterey/San Benito Counties' HMIS Planning and Oversight Committee, comprised of representatives from Partner Agencies and CHSP, is responsible for oversight and guidance of the Monterey/San Benito Counties' HMIS Project. This group is committed to balancing the interests and needs of all stakeholders involved: homeless men, women, and children; service providers; and policymakers.

Potential benefits for homeless men, women, children, and case managers:

Service coordination can improve when information is shared, with written client consent, among case management staff or with staff in other agencies serving the same clients.

Potential benefits for agencies and program managers:

Aggregated information can develop a complete understanding of clients' needs and outcomes and then advocate for additional resources, complete grant applications, conduct evaluations of program services, and report to funding agencies, such as HUD.

Potential benefits for the community-wide Continuum of Care (CoC) and policymakers:

County-wide involvement in the project provides the capacity to generate HUD annual progress reports for the Continuum of Care (CoC). It allows access to aggregate information, both at the local and regional level, that will assist in the identification of gaps in services. In addition, it will help the completion of other service reports used to inform policy decisions aimed at addressing and ending homelessness at local, state, and federal levels.

Governing Principles

Described below are the general governing principles upon which all decisions about the Monterey/San Benito counties' HMIS Project are based.

CHSP expects participants to read, understand, and adhere to the spirit of these governing principles, even when the Governance Policies and Procedures do not provide specific direction.

Confidentiality

The rights and privileges of clients are crucial to the success of HMIS. These policies will ensure clients' privacy without impacting the delivery of services. This is the primary focus of agency programs participating in this project. Policies regarding client data will be founded on the premise that clients own their personal information and provide the necessary safeguards to protect client, Agency, and policy level interests. The procedures outlined in this document will only permit the collection, access, and disclosure of client data through HMIS.

Data Integrity

Client data is the most valuable and sensitive asset of the Monterey/San Benito Counties' HMIS Project. These policies will ensure the integrity of client information and protect this asset from accidental or intentional unauthorized modification, destruction, or disclosure.

System Availability

The availability of a centralized data repository is necessary to achieve the ultimate CoC-wide aggregation of unduplicated homeless statistics. In addition, CHSP staff is responsible for ensuring the broadest deployment and availability for homeless service agencies in Monterey and San Benito Counties.

Compliance

Violation of the Governance Policies and Procedures outlined in this document will have serious consequences. Any deliberate or unintentional action resulting in a breach of confidentiality or loss of data integrity may result in the withdrawal of system access for the offending entity.

Roles and Responsibilities

Monterey and San Benito Counties' HMIS Planning and Oversight Committee

- Project direction and guidance
- Technology plan
- Selection of system software
- Approval of project forms and documentation
- Project participation and feedback
- Project Funding

Coalition of Homeless Services Providers (CHSP)

CHSP Executive Officer

- Liaison with the Department of Housing and Urban Development (HUD) and other state/federal partners.
- Project staffing
- CHSP signatory for Memoranda of Understandings
- Overall responsibility for the success of the Monterey/San Benito Counties' HMIS Project
- Policies & Procedures compliance
- General responsibility for project rollout

CHSP Staff – assigned HMIS duties (as applicable)

- End-user licenses
- Creation of project forms and documentation
- Keeper of signed Memorandums of Understanding
- User administration
    - Add and remove Partner Agency HMIS Administrators.
    - Manage user licenses
- Training Coordination for:
    - Curriculum development
    - Training documentation
    - Confidentiality training
    - Application training for HMIS Administrators and end-users
    - Outreach/End-user support
    - Training timetable
    - End-User Training
    - Helpdesk
    - Security Training
- Adherence to HUD data standards
- HMIS Lead Security Administrator
- Application customization
- Data monitoring
- Data validity
- Aggregate data reporting and extraction
- Assist Partner Agencies with agency-specific data collection and reporting needs (within reason and constraints of other duties).
- Data for annual US Dept. of HUD Continuum of Care Application Narrative
- Data collection and coordination of annual HUD Housing Inventory Count and sheltered Point in Time Count
- Liaison with WellSky
- Sign and manage the contractual agreement with WellSky
- Manage the implementation and ongoing usage of the HMIS system on behalf of the entire region

- Escalate problems to the application software vendor and hosting service provider, when necessary

WellSky

- Setup, operations, and ongoing maintenance of the HMIS system.
- Work with CHSP to plan and implement the system.
- Ensure CHSP receives appropriate training required for implementation and ongoing outreach and support.
- Provide technical assistance to the Continuum of Care HMIS Administration teams. Facilitate problem resolution in the event continuums are experiencing difficulties with the software and system. Resolve issues that the local Continuum of Care HMIS Administration could not adequately resolve.
- Perform application administration tasks as necessary for the setup and ongoing operations of the system
- Centrally manage the system-wide configuration on behalf of the multiple Continuums of Care, including:
    - Initial application setup and the first level, cross-continuum structure within the system.
    - Configuration of standard picklists provided with the product.
    - Configuration of standard client assessments provided with the product.
    - Procure, allocate and administer user license allocation across the various continuums within the system.
    - In coordination with the local Continuum of Care HMIS Administration, create and manage agency-specific application configurations on behalf of individual agencies within the system and include client assessment forms, data fields, and pick lists.
    - In coordination with local Continuum of Care HMIS Administration, advise on the creation and management of all custom data importation and exportation routines necessary to integrate external data into the HMIS system and export internal data from within the HMIS system, as required on behalf of individual agencies, Continuums of Care, or other outside policymakers and funders; such as the potential inclusion of HMIS data in a broader regional data warehouse. Audit usage of the application to ensure that appropriate standard Governance Policies and Procedures are agreed upon, in place, and followed.
    - Monitor system usage regularly to ensure that appropriate capacity planning is in place to proactively plan for future system growth and expansion.
- Follow all established Monterey and San Benito Counties' HMIS Project procedures, primarily procedures related to maintaining confidentiality.

Partner Agency

Partner Agency Executive Director

- Authorizing agent for partner agreement (MOU)
- Designation of HMIS Security Administrator and Agency Administrator
- Perform background checks on anyone designated as an HMIS Administrator
- Ensuring agency compliance with Governance Policies & Procedures
- End-user license management
- Agency level HUD reporting, if applicable

- Create and follow Agency Client Grievance Policy/Procedure as it relates to HMIS

Partner Agency Technical Administrator

- Overseeing agency compliance with the Memorandum of Understanding and all applicable plans, forms, standards, and governance documents
- Detecting and responding to violations of any applicable HMIS plans, forms, standards, and governance documents,
- Serving as the primary contact for all communication regarding the HMIS at this Agency and forwarding information to all Agency End-Users as appropriate,
- Ensuring thorough and accurate data collection by agency End-Users as specified by HMIS forms and standards,
- Providing first-level End-User support,
- Managing End-User licenses,
- Ensuring the Agency provides and maintains adequate internet connectivity,
- Maintaining Agency and program descriptor data in HMIS,
- Configuring provider preferences (assessments, referrals, services, etc.) in HMIS,
- Completing agency-level HUD reporting and supporting agency programs with reporting needs, if applicable,
- Ensuring all users adhere to the training(s) provided by CHSP
- Performing authorized imports of client data.

Partner Agency Security Officer

- Conducting a thorough bi-annual review of internal compliance with all applicable HMIS plans, standards, and governance documents
- Completing the Compliance Certification Checklist and forwarding the Checklist to CHSP,
- Continually monitoring and maintaining the security of all staff workstations used for HMIS data entry,
- Safeguarding client privacy by ensuring End-User and agency compliance with confidentiality and security policies,
- Investigating potential breaches of HMIS system security and client confidentiality and notifying CHSP of substantiated incidents,
- Developing and implementing procedures for managing new, retired, and compromised local system account credentials,
- Developing and implementing procedures that will prevent unauthorized users from connecting to private agency networks,
- Ensure all Agency End-Users complete the HMIS End-User Agreement and maintain documentation of all HMIS End-User Agreements,
- Ensure all Agency End-Users complete mandatory training and forward training documentation to the HMIS Lead Agency.

Partner Agency Staff

- Safeguard client privacy through compliance with confidentiality policies
- Data collection as specified by CHSP training, workflow charts, and other documentation

HMIS Participation Policy

Agencies participating in the Monterey/San Benito Counties' HMIS Project shall commit to abide by the governing principles of the Monterey/San Benito Counties' HMIS Project and adhere to the terms and conditions of this partnership as detailed in the memorandum of understanding.

Mandated Participation

All projects authorized under HUD's McKinney-Vento Act, as amended by the HEARTH Act to provide homeless services, must meet the minimum HMIS participation standards defined by this Policies and Procedures manual. In addition, these participating agencies will be required to comply with all applicable operating procedures and must agree to execute and abide by an HMIS Agency Partner Agreement.

Voluntary Participation

Although funded agencies must meet only minimum participation standards, CHSP strongly encourages funded agencies to participate in their homeless programs fully.

While CHSP cannot require non-funded providers to participate in the HMIS, CHSP works closely with non-funded agencies to articulate the benefits of the HMIS and strongly encourage their participation to achieve a comprehensive and an accurate understanding of homelessness in Monterey and San Benito Counties.

Minimum Participation Standards

- The Partner Agency shall confirm its participation in the Monterey/San Benito counties' HMIS Project by submitting a Memorandum of Understanding (MOU) to the CHSP Executive Officer.
- Agency staff shall collect the universal and program-specific data elements defined by HUD and other data elements as determined by the HMIS Oversight Committee for all clients served by programs participating in HMIS; agencies may share data with other agencies subjected to appropriate client consent and network data-sharing agreements.
- Agency staff shall enter client-level data into the HMIS within 72 hours or three business days of client interaction.
- Participating agencies shall comply with all HUD regulations for HMIS participation.

- Each Agency shall designate at least one HMIS Primary Point Person. This person may or may not also be the Agency Administrator (see below). The HMIS Primary Point Person functions as the principal liaison with CHSP Staff and is responsible for organizing its Agency's users, ensuring proper training has taken place for the users, and that all users from that Agency are following all paperwork and confidentiality requirements.
- Each Agency having five or more users must designate at least one user to function as an Agency Administrator. Agencies with fewer than five users can appoint an Agency Administrator. The Agency Administrator's role is to provide on-site support to the Agency's end-users, run agency reports, monitor the Agency's data quality, and work with CHSP Staff to troubleshoot HMIS issues. Agency Administrators are expected to attend HMIS User Group meetings.
- Each HMIS participating project within an agency must have a representative at each HMIS User Group meeting who can effectively communicate what is covered in the meeting to the rest of the project's HMIS users.

UPDATED 2022: HMIS License Cost and Billing

- HMIS Licenses cost **$445.00 per license/per year**. This fee is from our vendor, WellSky, and can change at their discretion. Once paid, your agency will own the license for the year and can transfer it to users as needed. If additional licenses are required after, agencies will be charged a prorated rate, and the license will expire annually at the end of **August**.
- **From August 2022 to August 2023 CHSP will subsidize each license by 50%**, as long as funding is available.
- Starting in August 2022 each agency will be billed **$222.50 per license.** CHSP will continue to search for funding to cover license fees.
- CHSP reserves the right to pull licenses that have not been used in over 90 days if funding is limited (See Rescinding User Access)

HMIS Partnership Termination

In the event the relationship between the CHSP HMIS and a Partner Agency is terminated, the Partner Agency will no longer have access to the HMIS.

Voluntary Termination

1. The Partner Agency shall inform the CHSP Executive Officer in writing of their intention to terminate their agreement to participate in Monterey/San Benito Counties' HMIS Project.
2. The CHSP Executive Officer will inform relevant CHSP staff, who will update the Participating Agency List.
3. The CHSP Executive Officer will revoke access of the Partner Agency staff to the Monterey/San Benito Counties' HMIS.
4. The CHSP Executive Officer will keep all termination records on file with the associated Memorandums of Understanding.

Lack of Compliance

If the CHSP Executive Officer, CHSP HMIS System Administrator, or CHSP Administrative Officer determines that a Partner Agency violates the terms of the partnership, Executive Directors of the Partner Agency and CHSP will strive to resolve the compliance issue(s) within 30 days of the conflict(s).

- If Executive Directors cannot resolve the compliance issue(s) within 30 days, the Peer Review Process will be employed to resolve the conflict if that results in a ruling of termination.
- The Partner Agency will be notified in writing of the intention to terminate its participation in the Monterey/San Benito Counties' HMIS Project. The CHSP Executive Officer will revoke access of the Partner Agency staff to the Monterey / San Benito Counties' HMIS.

Data Transfer Policies

CHSP Staff shall make reasonable accommodations to assist a Partner Agency in exporting its data in a usable format in its alternative database.

- Any costs associated with exporting the data will be the sole responsibility of the Partner Agency.
- All Partner Agency-specific information in the HMIS system will remain in the HMIS system.
- If the Agency's funder mandates HMIS participation, CHSP Executive Officer will remind Agency, either via email or mail, that terminating their participation will result in notification to the funder.

HMIS Agency Implementation

Adding Partner Agencies before setting up a new Partner Agency within the HMIS database, CHSP Staff shall:

- Review HMIS records to ensure that the Agency does not have previous violations
- Verify that the required documentation has been correctly executed and submitted or viewed on-site, including:
    - Partner Agreement
    - Additional Documentation on Agency and Project(s)
    - Designation of HMIS Primary Point Person/Agency Administrator
    - Coordinate License Fee Payment, if applicable
    - Request and receive approval from CHSP Staff to set up a new agency in the HMIS
    - Work with the Partner Agency to input relevant agency and program information
    - Work with CHSP Staff to migrate legacy data, if applicable Agency Information Security Protocol Requirements

At a minimum, Partner Agencies must develop security rules, protocols, or procedures based on the final HUD Data and Technical Standards, including but not limited to the following:

- Internal agency procedures for complying with the HMIS Notice of Privacy Practices and provisions of other HMIS client and Agency agreements
- Maintaining and posting an updated copy of the Agency's Notice of Privacy Practices on the Agency's website.
- Posting a sign in the areas of client intake that generally explains the reasons for collecting personal information
- Appropriate assignment of user accounts
- Preventing user account sharing

- Protection of unattended workstations
- Protection of physical access to workstations where employees are accessing HMIS
- Safe storage and secure access to hardcopy and digitally generated client records and reports with identifiable client information.
- Proper cleansing of equipment before transfer or disposal
- Procedures for regularly auditing compliance with the Agency's information security protocol

CHSP Staff will conduct annual site visits to monitor compliance with HMIS policies when agencies may need to demonstrate their procedures for securing client data. See HMIS Security Plan for more information.

User Access Levels

All HMIS users must be assigned a designated user access level that controls the level and type of access the user will have within the system. For example, users will have access to client-level data collected only by their Agency unless a client consents explicitly in writing to share their information.

Assignment of Agency HMIS Security and Technical Administrators

- The Partner Agency shall designate, in writing, an Agency HMIS Administrator for communications regarding Monterey/San Benito Counties' HMIS and submit this documentation to the CHSP Executive Officer.
- The CHSP staff will obtain all signatures necessary to execute the Partner Agency HMIS Administrator Agreement.
- The CHSP staff will maintain a file of all submitted documentation.
- The CHSP staff will maintain a list of all assigned Agency HMIS Administrators and make it available to the CHSP project staff.
- The Partner Agency may designate new or replacement Agency HMIS Administrators in the same manner as above.

User Authorization and Passwords

- Agency Staff participating in the Monterey/San Benito Counties' HMIS Project shall commit to abide by the governing principles of the Monterey/San Benito Counties' HMIS Project and adhere to the terms and conditions of the Partner Agency User Agreement.
- The Partner Agency HMIS Administrator must only request user access to HMIS for those staff members that require access to perform their job duties.
- All users must have their own unique User ID and should never use or allow the use of a user ID that is not assigned to them. [See Partner Agency User Agreement]
- All users must have their own unique email address that includes the agency's domain name in the address. For example, **user@chsp.org** , "**chsp.org**" would be the agency's domain name.
- Temporary passwords will be communicated via email to the owner of the User ID.
- User-specified passwords should never be shared and communicated in any format.
- New User IDs must require password change on first use.

- Passwords must consist of 8 to 16 characters and must contain a combination of letters and numbers (no special characters, alpha and numeric only). The password must contain at least two digits. [Required by software.] According to the HUD Data Specification Draft:

User authentication. HMIS workstations and servers shall be secured with, at a minimum, a user authentication system consisting of a username and a password. Passwords shall be at least eight characters long and meet industry standard complexity requirements, including, but not limited to, the use of at least one of each of the following kinds of characters in the passwords: Upper and lower-case letters, and numbers, and symbols. Passwords shall not be, or include, the username, the HMIS name, or the HMIS vendor's name. In addition, passwords should not consist entirely of any word found in the standard dictionary or any of the above spelled backward. The use of default passwords on initial entry into the HMIS application is allowed so long as the application requires that the default password be changed on first use. Written information specifically about user access (e.g., username and password) shall not be stored or displayed in any publicly accessible location.

- Passwords must be changed every 45 calendar days. If they are not changed within that period, they will expire, and the user will be locked out of the system.
- For Agency Users (not including Partner Agency HMIS Administrator), passwords can be reset by clicking the "Forgot Password" link on the ServicePoint (HMIS) login screen.
- Three consecutive unsuccessful login attempts will disable the User ID until an administrator reactivates the account.
- Personal devices are not permitted to access HMIS.
- Users who have not attended HMIS New User training in more than one year have to undergo training before activating their license when transitioning to a new~~s~~ agency.
- CHSP or the Partner Agency Admin must activate end-user licenses within 90 days of training. Users who do not have their licenses activated within the said timeframe will have to re-attend New User training.
- New users must participate in the annual security training. Users who do not renew will be locked out until completed.

HMIS Security Plan

The Continuum has defined a security plan that:

- Ensures the confidentiality, integrity, and availability of all HMIS information
- Protects against any reasonably anticipated threats or hazards to the security
- Ensures compliance by end-users

Security Plan Overview

- The Partner Agency Security Officer is responsible for preventing degradation of the HMIS resulting from viruses, intrusion, or other factors within the Agency's control~~.~~
- The Partner Agency Security Officer is responsible for preventing the inadvertent release of confidential client-specific information through physical, electronic, or visual access to the workstation~~.~~

- Each Partner Agency is responsible for meeting 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 quarterly.
- The HMIS System Administrator will promote the security of HMIS and the confidentiality of the data contained therein; access to HMIS will be available only through approved workstations.
- End-Users shall commit to abide by the governing principles of HMIS and adhere to the terms and conditions of the HMIS End-User Agreement.
- CHSP will provide an appropriate level of HMIS access to individuals who require access to perform their assigned duties on behalf of an HMIS Partner Agency.
- User IDs are individual, and passwords are confidential. No individual should ever use or allow the 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.

HMIS Security Roles

Security Officers

The HMIS Lead Agency and all HMIS Partner Agencies must designate Security Officers to oversee HMIS privacy and security.

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 and is adequately skilled to assess HMIS security compliance,
- Assesses security measures in place before establishing access to HMIS for a new Partner 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 Technical Administrator or another Partner Agency employee, volunteer, or contractor who has completed HMIS Privacy and Security training and is adequately skilled in assessing HMIS security compliance
- Conducts a security audit for any workstation that will be used for HMIS data collection or entry
  - No less than quarterly for all Agency HMIS workstations, AND
  - Before 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 Quarterly Compliance Certification Checklist and forwards the Checklist to the Lead Security Officer

Security Audits

New HMIS Partner Agency Site Security Assessment

Before 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), Partner Agency HMIS Technical Administrator, and Partner Agency Security Officer to review the Partner Agency's information security protocols before 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 complete responsibility of the Partner Agency, it's Executive Director, and its Technical Administrator/Security Officer.

Quarterly Partner Agency Self-Audits

1. The Partner Agency Security Officer will use the Compliance Certification Checklist to conduct quarterly security audits of all Partner Agency HMIS End-User workstations.
2. The Partner Agency Security Officer will audit remote access by associating User IDs, IP addresses, and login date/times with employee timesheets. End-Users may not remotely access HMIS from a workstation (i.e., personal computer) that is not subject to regular audits by the Partner Agency Security Officer.
3. Suppose areas are identified that require action due to non-compliance with these standards or any element of the Monterey and San Benito Counties HMIS Policies and Procedures. In that case, the Partner Agency Security Officer will note these on the Compliance Certification Checklist, and the Partner Agency Security Officer and HMIS Technical Administrator will work to resolve the action item(s) within one month.
4. Any Compliance Certification Checklist that includes one or more findings of non-compliance and action items will not be considered valid until all action items have been resolved. The Checklist findings, action items, and resolution summary must be reviewed and signed by the Partner Agency Executive Director or other empowered officers before being forwarded to the Lead Security Officer.
5. The Partner Agency Security Officer must turn in a copy of the Compliance Certification Checklist to the Lead Security Officer every quarter.

Annual Security Audits

1. The Lead Security Officer will schedule the annual security audit in advance with the Partner Agency Security Officer.
2. The Lead Security Officer will use the Compliance Certification Checklist to conduct security audits.

3. The Lead Security Officer must randomly audit at least 10% of the workstations for each HMIS Partner Agency. In the event that an agency has more than one program site, at least one workstation per program site must be audited.
4. The HMIS System Administrator should note each compliance check for each computer in the compliance Checklist.
5. Suppose areas are identified that require action due to non-compliance with these standards or any element of the Monterey and San Benito Counties HMIS Policies and Procedures. In that case, the Lead Security Officer will note these on the Compliance Certification Checklist. The Partner Agency Security Officer or Technical Administrator will work to resolve the action item(s) within one month.
6. Any Compliance Certification Checklist that includes one or more findings of non-compliance or action items will not be considered valid until all action items have been resolved. In addition to the Checklist findings, action items, and resolution summary being reviewed and signed by the Partner Agency Executive Director or other empowered officer and forwarded to the HMIS Lead Security Officer.

Physical Safeguards

In order to protect client privacy, the following physical safeguards must be put in place. For this section, authorized persons will be considered only those individuals who have completed 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 HMIS workstation must not be accessible to clients, the public, or other unauthorized Partner Agency staff members or volunteers.
- Printer location – Documents printed from HMIS must be sent to a printer in a secure area 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.

Technical Safeguards

Workstation Specification

- Partner Agency HMIS Administrator is responsible for taking the necessary actions to prevent the degradation of the whole system resulting from viruses, intrusion, or other factors under the Agency's control.
- Partner Agency HMIS Administrator is responsible for preventing the inadvertent release of confidential client-specific information. Such release may come from physical, electronic, or even visual access to the station; thus, steps should be taken to prevent these modes of inappropriate access (i.e., don't let someone read over your shoulder; lock your screen).
- Recommended Internet Connection: At minimum, DSL
- Recommended Browser: Latest release of Internet Explorer, Chrome, Firefox, or Opera

- Definition and communication of all procedures to all agency users for achieving proper agency workstation configuration and for protecting their access by all agency users to the broader system are the responsibility of the Partner Agency HMIS Administrator.
- Workstations should be password protected and locked when not in use.

Workstation Security

1. 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).
2. Partner Agency Security Officer will confirm that any workstation accessing HMIS has and uses a hardware or software firewall.

Establishing HMIS User IDs and Access Levels

1. The Partner Agency Technical Administrator will ensure that any prospective End-User reads, understands, and signs the HMIS End-User Agreement.
2. The Partner Agency Technical Administrator is responsible for ensuring that all Agency End-Users have completed mandatory training, including HMIS Privacy, Security and Ethics training and End-User Responsibilities and Workflow training, before being provided with a User ID to access HMIS.
3. The Partner Agency Technical Administrator will maintain a file of all signed HMIS End-User Agreements.
4. All End-Users will be issued a unique User ID and password. Sharing 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.
5. The Partner Agency Technical Administrator will always attempt to assign the most restrictive access that allows the End-User to efficiently and effectively perform their assigned duties.
6. The Partner Agency Technical Administrator will create the new User ID and notify the User ID owner of the temporary password verbally via telephone or in-person.
7. When the Partner Agency Technical Administrator determines that it is necessary to change a user's access level, the Partner Agency Technical Administrator will update the user account as necessary.

Passwords

1. Temporary passwords must be changed on first use. User-specified passwords must be a minimum of 8 characters long and must contain a combination of letters and at least two numbers.
2. The software will prompt End-Users to change their passwords every 45 days.
3. End-Users must immediately notify their Partner Agency Technical Administrator if they have reason to believe that someone else has gained access to their password.

4. Three consecutive unsuccessful attempts to log in will disable the User ID until the password is reset. For Agency End-Users (not including Partner Agency Technical Administrators), passwords should be reset by the Partner Agency Technical Administrator but, in some cases, may be reset by the HMIS System Administrator. For Partner Agency Technical Administrators, passwords may only be reset by the HMIS System Administrator.

Rescinding User Access

1. The Partner Agency Technical Administrator should terminate end-User access within 24 hours if an End-User no longer requires access to perform their assigned duties due to a change of job duties or termination of employment.
2. The HMIS System Administrator reserves the right to terminate End User Licenses with 90 days or more of inactivity. While users will not be kicked until they reach 90 days of inactivity, CHSP maintains the discretion to revoke inactive licenses after 45 days if the CoC is experiencing a shortage of licenses. It is therefore recommended that users log in and utilize their allocated licenses regularly to avoid having their privileges revoked.
3. The HMIS System Administrator will attempt to contact the Partner Agency Technical Administrator for the End User in question before the inactive user license is terminated.
4. In the event of suspected or demonstrated non-compliance by an End User with the HMIS End User Agreement or any other HMIS plans, forms, standards, or governance documents, the Partner Agency Technical Administrator should deactivate the User ID for the End User in question until an internal agency investigation has been completed. The Partner Agency Technical Administrator or Partner Agency Security Officer shall notify the HMIS Lead Agency of any substantiated incidents that may have resulted in a breach of HMIS system security or client confidentiality, whether or not a breach is definitively known to have occurred.
5. Suppose the Partner Agency Technical Administrator is unable or unwilling to do so. In that case, the HMIS System Administrator will deactivate User IDs pending further investigation if an End User's non-compliance with the HMIS End User Agreement is suspected or demonstrated.
6. The Continuum of Care is empowered to permanently revoke a Partner Agency's access to HMIS for substantiated non-compliance with the provisions of these Security Standards, the Monterey and San Benito Counties HMIS Policies and Procedures, or the Partner Agency Privacy Statement that resulted in a release of Personal Protected Information (PPI).

Other Technical Safeguards

The HMIS software vendor currently implements most other technical safeguards for the Monterey and San Benito Counties HMIS.

1. The Lead Security Officer shall develop and implement procedures for managing new, retired, and compromised HMIS account credentials.
2. The Partner Agency Security Officer shall develop and implement procedures for managing new, retired, and compromised local system account credentials.
3. The Partner Agency Security Officer shall develop and implement procedures to prevent unauthorized users from connecting to private agency networks.

4. 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 an agency shared drive. All PPI downloaded files must be deleted from the temporary workstation files and the "Recycling Bin" emptied before the End User leaves the workstation.

Workforce Security

The HMIS Lead Agency will ensure background checks are conducted on all individuals to be designated as a Lead Security Officer or HMIS System Administrator.

1. The background check results must be considered on a case-by-case basis to protect the security and integrity of the HMIS system and safeguard the personal information contained therein. An individual whose background indicates that they may not sufficiently be relied upon to help achieve this goal may not be given administrative-level access to HMIS.
2. The background check results must be retained in the subject's personnel file.
3. A background check may be conducted only once for each person unless otherwise required.

Reporting Security Incidents

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

1. Any HMIS End User who becomes aware of or suspects a compromise of HMIS system security and/or client privacy must immediately report that possible incident to the Partner Agency Security Officer.
2. If there is a suspected security compromise, the Partner Agency Security Officer should complete an internal investigation. If the alleged compromise resulted from an End User's suspected or demonstrated non-compliance with the HMIS End User Agreement, the Partner Agency Security Officer should deactivate the End User's User ID until the internal investigation has been completed.
3. Following the internal investigation, the Partner Agency Security Officer shall notify the Lead Security Officer of any substantiated incidents that may have resulted in a breach of HMIS system security or client privacy, whether or not a breach is definitively known to have occurred. Suppose the violation resulted from demonstrated non-compliance by an End User with the HMIS End User Agreement. In that case, the Lead Security Officer reserves the right to permanently deactivate the User ID for the End User in question.
4. Within one business day after the Lead Security Officer receives notice of the breach, the Lead Security Officer and Partner Agency Security Officer will jointly establish an action plan to analyze the source of the violation and actively prevent future violations. The action plan shall be implemented as soon as possible, and the full term of the plan must not exceed 30 days. Suppose the Partner Agency cannot meet the terms of the action plan within the time allotted. In that case, the HMIS System Administrator, in consultation with the Monterey and San Benito Counties Continuum of Care Ombudsperson, may elect to terminate the Partner Agency's access

to HMIS. However, the Partner Agency may appeal to the Ombudsperson for reinstatement to HMIS following completion of the requirements of the action plan.

5. In the event of a substantiated breach of client privacy through a release of Personal Protected Information (PPI) in non-compliance with the provisions of these Security Standards, the Monterey and San Benito Counties HMIS Policies and Procedures, or the Partner Agency Privacy Statement, the Agency Security Officer will attempt to notify any impacted individual(s).
6. The HMIS Lead Agency will notify the appropriate body of the Continuum of Care of any substantiated release of Personal Protected Information (PPI) in non-compliance with the provisions of these Security Standards, the Monterey San Benito Counties HMIS Policies and Procedures, or the Partner Agency Privacy Statement.
7. The HMIS Lead Agency will maintain a record of all substantiated releases of Personal Protected Information (PPI) in non-compliance with the provisions of these Security Standards, the Monterey and San Benito Counties HMIS Policies and Procedures, or the Partner Agency Privacy Statement for seven years.
8. The Continuum of Care reserves the right to permanently revoke a Partner Agency's access to HMIS for substantiated non-compliance with the provisions of these Security Standards, the Monterey and San Benito Counties HMIS Policies and Procedures, or the Partner Agency Privacy Statement that resulted in a release of Personal Protected Information (PPI).

Disaster Recovery Plan

Disaster Recovery for the Monterey and San Benito Counties HMIS will be conducted by the CHSP HMIS System Admin in collaboration with the HMIS vendor WellSky.

1. The Lead Security Officer should maintain ready access to the following information:
    a) Contact information – Phone number and email address of the Bowman Systems contact responsible for recovering the Agency's data after a disaster.
    b) Agency responsibilities – A thorough understanding of the Agency's role in facilitating recovery from a disaster.
    c) 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.
2. 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.
    a) Account information – Account numbers and contact information for the internet service provider, support contracts, and equipment warranties.
    b) 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.
    c) Network and system configuration information – Documentation of the configuration settings required to restore local user accounts and internet access.

Collection and Entry of Client Data

Partner Agencies will solicit or enter information about clients into the HMIS database only to provide services or conduct evaluation or research. In consultation with CHSP, Partner Agency management will determine what qualifies as essential for assistance or analysis.

- Client data will be gathered according to each program's policies, procedures, and confidentiality rules.
- Client data may only be entered into the HMIS with the client's authorization to do so.
- Client data will only be shared with Partner Agencies if the client consents by signing the client consent form, and that form is filed on record.
- Client data will be entered into the HMIS promptly.
- Client identification should be completed during the intake process or as soon as possible following the intake within 72 hours or three business days.
- Service records should be entered on the day services began or as soon as possible within the next 72 hours or three business days.
- Required assessments should be entered as soon as possible following the intake process and within 72 hours or three business days.
- All client data entered into the HMIS will be kept as accurate and current as possible.
- Hardcopy and electronic files will continue to be maintained according to individual program requirements under the HUD Data Standards.
- Data may not be imported without the client's authorization.
- Any authorized data imports will be the responsibility of the participating Agency.
- Partner Agencies are responsible for the accuracy, integrity, and security of all data input by said Agency.
- Partner agencies must adhere to workflows provided by CHSP. Changes to workflows must be submitted in writing to the CHSP and will be brought to the Oversight Committee for final approval.
- Victim Service Providers (VSPs) are prohibited from entering data into HMIS. Non-VSP agencies must offer clients fleeing domestic violence the opportunity to have their information entered into HMIS locked down. If the client's profile already exists, the new program entry should be locked down. If the client is new to HMIS, the entire profile should be locked down.
- Agencies that lockdown any clients must report the client ID to CHSP via webform so that CHSP can manage all locked client data.

HMIS Data Quality Plan

The Continuum has defined a data quality plan that:

- Is based on HUD data standards and CoC data requirements, all participating agencies specify the data quality standard to be used.
- Provides a mechanism for monitoring adherence to the standard
- Provides the necessary tools and training to ensure compliance with the standard

- Includes strategies for working with agencies that are not in compliance with the standard

HMIS Data Collection

Data Quality Standard

- All data entered will be accurate.
- Per HUD data standards, blank entries in required data fields will not exceed 5% per month.
- All services provided will be compatible with the program.
- Data entry, including program Entry and Exit transactions, must be complete within five working days of data collection.

Data Quality Monitoring

The HMIS Management Team will perform regular data integrity checks on the HMIS data. Any patterns of error at a Partner Agency will be reported to the Agency Administrator or Primary Point Person. When patterns of the error are discovered, users are required to correct data entry techniques and will be monitored for compliance.

Partner Agencies are expected to:

- Run and submit data completeness reports, data incongruities reports, and other data quality reports as required by HMIS Lead staff
- Review monthly PIT reports confirming accurate program entry and exit data.
- Notify HMIS Lead staff of findings and timelines for correction
- Rerun reports for errant agencies/programs to confirm data correction
- Create a notification for Agency Executive Director and submit it to HMIS Lead staff for approval

Data Collection Requirements

Required Data Elements

A Partner Agency is responsible for ensuring that a minimum set of data elements, referred to as the Universal Data Elements (UDEs) and Program-specific Data Elements as defined by the HUD Data and Technical Standards, and other data elements as determined by the HMIS Committee will be collected and verified from all clients at their initial program enrollment or as soon as possible after that. Partner Agencies must enter data into the HMIS within five business days of collecting the information.

These required data elements are included collectively on the Client Profile, Client Demographics section, Comprehensive Entry, and Interim and Review assessments. In addition, they have a timely entry of program Entry and Exit transaction data.

Partner Agencies must report client-level UDEs and Program-specific Data Elements using the required response categories detailed in the HUD Data and Technical Standards. These standards are already incorporated into the HMIS.

Entry/Exit Data

Agencies should record program entry and exit dates upon any program entry or exit on all participants. Entry dates should record the first day of service or program entry with a new program entry date for each period/episode of service. Exit dates should record the last day of residence in a program's housing before the participant leaves the shelter or if the Agency provided a service the previous day.

Data Quality Training Requirements

End-User Training

Each end-user of the HMIS system must complete Alliance-approved HMIS training before being given HMIS login credentials. In addition, it is recommended that they also receive training from their Agency Administrator to understand agency-specific nuances in how they enter data. HMIS Primary Point Persons and Agency Administrators should notify the Alliance when specific training needs are for their end-users.

Reports Training

Reports training for Agency Administrators and other interested users will be made available as needed. These will include training on how to use Provider Reports in ServicePoint, how to use ReportWriter to create simple reports, how to run existing reports in the Advanced Reporting Tool (ART), and may include opportunities for training.

HMIS De-Duplications of Data

De-duplicating Data Elements

The HMIS application will use the following data elements to create unduplicated client records:

- Name (first, middle, last, suffix; aliases or nicknames should be avoided unless the client is fleeing DV)
- Social Security Number
- Date of Birth (actual or estimated)
- Gender
- Race and Ethnicity

User-mediated Look-up

The primary way to achieve de-duplication will be a user-mediated search of the client database before creating a new client record. ClientPoint will prompt the user to enter a minimum number of

data elements into the HMIS application, and a list of similar client records will be displayed. The user will be asked to select a matching record if the other identifying fields match correctly based on the results. Suppose the user is unsure of a match (either because some data elements differ or blank information). In that case, the user should query the client for more details and continue evaluating possible matches or create a new client record. The user will not be able to view sensitive client information or program-specific information during the de-duplication process. After the client record is selected, the user can only view previously existing portions of the client record if they have explicit authorization to view that client's history.

Back-end Central Server Matching Based on Identifiable Information

When Primary Identifiers are not shared across agencies for de-duplication purposes, CHSP Staff, with the assistance of the Agency Administrator, will manage a process for matching a client's personal identifying information based on a Unique Client ID that the HMIS assigns to each client. The Unique Client ID provides an unduplicated internal count of clients served by the Agency and provides CHSP Staff with a longitudinal analysis of services provided to each client.

Release and Disclosure of Client Data

Each HMIS Partner Agencies must comply with the following uses and disclosures, as outlined in the HUD Data and Technical Standards: Notice for Uses and Disclosures for Protected Personal Information (PPI). A Partner Agency has the right to establish additional uses and disclosures as long as they do not conflict with CHSP-approved uses and disclosures.

Privacy Notice Requirement

Each Partner Agency must publish a privacy notice that incorporates the content of the HUD Data and Technical Standards Notice as described below. Agencies that develop their own privacy and security policies must allow for the de-duplication of homeless clients at the Continuum level. Each Agency must post a privacy notice and provide a copy of the privacy notice to any client upon request. If an agency maintains a public web page, the Agency must post the current version of its privacy notice on its web page.

Release and Disclosure Requirements

- Client-specific data from the HMIS system may be shared with partner agencies only when the sharing Agency has secured a valid Release of Information Form (ROI) from that client authorizing such sharing and only during such time that release of information is valid (before its expiration). Other non- HMIS inter-agency agreements do not cover the sharing of HMIS data.
- Program-specific confidentiality rules may limit sharing of client data.
- No client-specific data will be released or shared outside of the partner agencies unless the client gives specific written permission, or withholding that information would be illegal. Please see the release of information.

- Partner Agencies may **not** deny services based on the client's refusal to sign the form or to state any information.
- Release of information must constitute **informed** consent. The burden rests with the intake counselor to inform the client before asking for consent. As part of informed consent, the relevant portions of these Governance Policies and Procedures, as well as privacy language found in the final HUD Data Standards, should be posted near the intake location or be available at the intake location, along with Agency's relevant Governance Policies & Procedures and a list of agencies participating in Monterey/San Benito Counties' HMIS Project.
- All approved notices are found on the CHSP website.
- The client shall be given a printout of all HMIS data relating to them upon written request and within 10 working days from when the written request is received. Written requests will be date/time stamped immediately upon receipt.
- A report of data sharing events, including dates, agencies, persons, and other details, must be made available to the client upon request within 10 working days from when the written request is received. Written requests will be date/time stamped immediately upon receipt.
- A log of all external releases or disclosures must be maintained for seven years and made available to the client upon written request within 10 working days from when the written request is received. Written requests will be date/time stamped immediately upon receipt.
- Aggregate data that does not contain any client-specific identifying data may be shared with internal and external agents without specific permission. This policy should be made clear to clients as part of the informed consent procedure.
- Each Agency Executive Director is responsible for the Agency's internal compliance with the HUD Data Standards.
- ROIs expire after three (3) years unless Partner Agencies' internal policies conflict with that timeline.
- End-Users do not use the client's name, DOB, or SSN via phone calls and emails but are to use the HMIS client ID number provided through ServicePoint.

Considerations for Client Consent

A. Consent to enter the essential and relevant information into the Homeless Management Information System (HMIS) during the time frame when the ROI is active and shared between partner agencies.
   a) The ROI permits visibility of the client's activity during which the ROI is active. After the ROI expires, the client's information will still be visible. Data entered into HMIS after the ROI expires against policy.

B. Consent to enter the essential and relevant information into HMIS during the time frame when the ROI is active but not shared between Partner Agencies.
   a) If the client already exists in HMIS, only the specific program Entry will be locked down to all users outside the receiving Agency.
   b) If the client did not already exist in HMIS, the entire client profile would be locked down to all users outside of the receiving Agency.

C. Altogether refuse to sign the ROI. (In this case, the Agency has the following options)

a) Ask the client to provide their alias and enter the client's information into HMIS (except for their social security number and birthday.) The Agency should record the client's alias in the client's folder. Many clients have street names and may choose to use that name. This practice is the most desirable option as the client is likely to remember this alias and use it at other agencies, reducing the possibility of double entry.
b) The Agency may have its own unique name (or alias) and enter the client's information into HMIS (except for their social security number and birthday.) The Agency should record the client's pseudonym in the client's folder.
c) Opt-out on entering the client's information into HMIS completely while remembering to manually include the client in all reporting (HIC/PIT, ESG, PATH, etc.)

Sub Population Considerations

Conflict Resolution Process for HMIS

Conflicts, grievances, etc., should be handled at the lowest level possible at every level of the Monterey/San Benito Counties' HMIS. Reasonable efforts should be made and documented, if possible and appropriate, to obtain satisfaction by other means, including escalation within an agency and through CHSP.

Client-level conflicts will be handled within the Partner Agency using its agency Client Grievance Policy/Procedure.

- All Partner Agencies will have a Client Grievance Policy/Procedure.
- Partner Agency Client Grievance Policy/Procedures are reviewed as they relate to the Monterey/San Benito Counties' HMIS by the HMIS Planning and Oversight Committee and CHSP Executive Officer for feedback and comments.

Changes to a Partner Agency Client Grievance Policy/Procedure will be submitted to the CHSP Executive Officer and HMIS Planning and Oversight Committee in writing within 30 days of the changes for feedback and comments.

Agency level conflicts will be handled through an escalating peer-review process:

- The CHSP Executive Officer, CHSP staff, Partner Agency Executive Director, or HMIS Agency Administrator will attempt to resolve conflicts as they occur. CHSP or the Partner Agency may annotate their concerns in writing as appropriate.

- Unresolved conflicts between the CHSP and a Partner Agency will be noted in writing and forwarded to the CHSP Executive Committee. In the event of an impasse, other board members will be notified within 10 working days of the impasse declaration. Either party may declare an impasse.
- The CHSP Executive Committee will review the written grievance at the next scheduled Executive Committee meeting. The Executive Committee will attempt to resolve the matter within 30 days of reviewing the grievance. Resolution of the conflict will be in writing and signed by all relevant parties.
- Unresolved conflicts will be forwarded to the full CHSP Board of Directors for further guidance and action.
- Any recommendation regarding the termination of a Partner Agency from the Monterey/San Benito Counties' HMIS will be forwarded to the full CHSP Board of Directors for consideration and possible action.
- All decisions of the CHSP Board of Directors are final.
- Conflicts between or among Partner Agencies may require mediation by the CHSP Executive Officer or CHSP staff. Resolution of the conflict may be annotated in writing and signed by all relevant parties as appropriate.

Unresolved conflicts between or among Partner Agencies will be noted in writing and forwarded to the CHSP Executive Committee within 10 working days of the date of an impasse. Any party may declare an impasse. The Executive Committee will then follow the same process noted above.

Training

Agency Executive Director shall obtain the commitment of the Agency HMIS Administrator and designated staff persons to attend training(s) as specified in the Memorandum of Understanding (MOU) between Partner Agency and CHSP. Changes to the Data Standards require mandatory user training. Therefore, users who do not attend will be temporarily locked out of HMIS until trained.

Required Trainings

Start-up Training

CHSP will provide or coordinate training in the following areas before Partner Agency using the Monterey/San Benito Counties' HMIS:

- Partner Agency HMIS Administrator Training
- New User Training

Agency HMIS Administrator Training

Training will be done in a group setting, where possible, to achieve the most efficient use of time and sharing of information between agencies. Training will include:

- HMIS Policies and Procedures
- New user setup procedures
- End-user training
- Running package reports
- Client Rights
- Technical and Security Administrator Duties
- Password Resets
- Data Quality

On-going Training

CHSP will provide regular training for HMIS End-Users on an as-needed basis. The areas covered will be:

- Confidentiality
- Data Quality
- Workflows
- Data Standards changes
- System upgrades

Additional training classes may be scheduled, as needed, under the guidance of the CHSP and HMIS Planning and Oversight Committee.

Compliance

Compliance with these Governance Policies and Procedures is mandatory for participation in the Monterey/San Benito Counties' HMIS system. Using the ServicePoint software, all changes to client data are recorded and will be periodically and randomly audited for compliance by CHSP staff.

Technical Support

Support requests for Technical Support might include problem reporting, requests for enhancements (features), or other general technical support. Users shall submit support requests to their Partner Agency HMIS Administrator or file a case. As random technical support questions on the use of the HMIS application arise, users will follow this procedure to resolve those questions:

During the normal business hours of CHSP:

- Begin with the utilization of the online help and training materials
- If the question is still unresolved, direct the technical support question to the Agency Administrator or Primary Point Person.
- If the question is still unresolved, the Agency Administrator or Primary Point Person can direct the inquiry to CHSP Staff.
- If the question is still unresolved, CHSP Staff will direct the inquiry to Bowman Systems technical support staff.

After the normal business hours of CHSP:

- Begin with the utilization of the online help and training materials
- If the question can wait to be addressed during the following business day, wait and follow the standard business hours procedure outlined above.
- If the question cannot wait, direct the technical support question to the Agency Administrator or Primary Point Person.
- If unavailable and the question is still unresolved, contact the HMIS Management Team or the duly appointed representative. They will determine the appropriate procedure to follow.

If it is determined that the issue needs immediate attention, the user's request will be forwarded to an appropriate WellSky HMIS technical support representative. Otherwise, the user will be instructed to pursue assistance through normal channels on the following business day.

- Users shall not, under any circumstances, submit requests to WellSky.
- Users shall not submit requests directly to CHSP via email or telephone.
- CHSP will only provide support for issues specific to the Monterey/San Benito Counties' HMIS Project software and systems.

Agency/User Forms

All Agency Administrators and Primary Point Persons will be trained in the appropriate online and hardcopy forms. If the Agency Administrator or Primary Point Person has questions on how to complete HMIS forms, they shall contact the HMIS Management Team.

Report Generation

Each Agency may send its Agency Administrator to receive training on developing agency-specific reports using the HMIS application. The HMIS Management Team will be a resource to agency users as they build reports but will be available to provide only a limited, reasonable level of support to

each Agency. The HMIS User Group will be the primary body to query Partner Agencies on their reporting needs and prioritize a list of reports developed by the Alliance for use by all Partner Agencies.

Programming-related Service Requests

If a user encounters programming issues within the HMIS application that needs a resolution, that user should identify the error or suggest an improvement to the Agency Administrator. The Agency Administrator will forward this information to the HMIS Management Team, recognizing the specific nature of the issue or recommended improvement, along with the immediacy of the request. The HMIS Management Team will review all application service requests and determine the action to be taken. Proposals to fix programming errors will be prioritized and forwarded to WellSky. Suggested application improvements will be compiled and periodically discussed by the HMIS Committee and the HMIS User Group. A prioritized list of improvements for review will be submitted to the HMIS Management Team. The HMIS System Administrator will submit approved recommendations to Bowman Systems.

Changes to this and other Documents

- The Monterey and San Benito Counties' HMIS Planning and Oversight Committee will guide the recommendations regarding the compilation and amendment of these Governance Policies and Procedures.
- The Governance Policies and Procedures must be reviewed and updated every year.
- Interim changes will be pre-approved by the Monterey and San Benito Counties' HMIS Planning and Oversight Committee. They will be added as an addendum until the next updating cycle of this document.
- A newly executed MOU should follow the implementation of any updated Governance Policies and Procedures.

Changes to Governance Policies & Procedures

1. Proposed changes may originate from any Monterey/San Benito counties' HMIS Project participant.
2. When proposed changes originate within a Partner Agency, they must be reviewed by the Partner Agency Executive Director and then submitted to the CHSP Executive Director for review and discussion.
3. CHSP staff will maintain a list of proposed changes.
4. The HMIS Planning and Oversight Committee will discuss the list of proposed changes, subject to line-item excision and modification. This discussion may occur either at a meeting of the group or via email or conference call, according to the discretion and direction of the group.
5. Results of said discussion will be communicated, along with the recommended amendment to the Governance Policies and Procedures.
6. Partner Agencies' Executive Directors shall acknowledge receipt and acceptance of the revised Governance Policies and Procedures within 10 working days of delivery of the amended

Governance Policies and Procedures by signing and returning this document to the CHSP Executive Officer.

7. Partner Agency Executive Director shall also ensure circulation of the revised document within their Agency and compliance with the revised Governance Policies and Procedures.

Attachment A: Definitions

Access Point: Locations where people can complete the standardized assessment to participate in Coordinated Entry. Access points often include emergency shelters and drop-in service centers.

At-Risk of Homelessness: An individual or family who has income below 30% of area median family income for the area, as defined by HUD, and who does not have sufficient resources or support networks immediately available to prevent them from moving into an emergency shelter or other place described in the "homeless" definition, and meets one of the following definitions defined under 24 CFR 578.3 (CoC program) or 24 CFR 576.2 (ESG program). This may also include a child or youth who qualifies as homeless under other Federal programs.

California Emergency Solutions and Housing (CESH): Provides funds for various activities to assist persons experiencing or at risk of homelessness as authorized by SB 850 (Chapter 48, Statues of 2018). The California Department of Housing and Community Development (HCD) administers the CESH Program with funding received from the Building Homes and Jobs Act Trust Fund (SB 2, Chapter 364, Statutes of 2017)

Chronically Homeless Individual (CHI): Under HUD's definition, "chronic homelessness" means an individual who lives either in a place not meant for human habitation, Safe Haven, or in an Emergency Shelter immediately before entering the institutional care facility.

- To meet the CHI definition, the individual must have been living as described above continuously for 12 months or on at least four separate occasions in the last three years, where the combined occasions total a length of at least 12 months. Each period separating the events must include at least seven nights of living in a situation other than a place not meant for human habitation in an Emergency Shelter or a Safe Haven.

Continuum of Care (CoC): The Monterey and San Benito Counties Continuum of Care carries out the responsibilities required under HUD regulations, outlined in 24 CFR 578 – Continuum of Care Program. The CoC consists of a broad group of stakeholders dedicated to ending and preventing homelessness in Monterey and San Benito Counties. CoC's overarching responsibility is to ensure community-wide

implementation of efforts to end homelessness and ensure programmatic and systemic effects of the local Continuum of Care program.

Diversion: A strategy that prevents homelessness for people seeking shelter by helping them identify immediate alternate housing arrangements and, if necessary, connecting them with services and financial assistance to help them return to permanent housing. Diversion programs can reduce the number of families facing homelessness, the demand for shelter beds, and the size of program waitlists.

Emergency Shelter: Any facility whose primary purpose is to provide a temporary shelter for the homeless in general or specific homeless populations and does not require occupants to sign leases or occupancy agreements.

Emergency Solutions Grant (ESG): ESG is a grant program of the HUD that funds emergency assistance for people who are homeless or at risk of homelessness. ESG grantees are required to participate in Coordinated Entry.

Categories of Homelessness: HUD's definition of homelessness (24 CFR 578.3) has four categories:

- Category 1 – Literally Homeless individuals/families
- Category 2 – Individuals/families who will imminently lose their primary nighttime residence with no subsequent residence, resources, or support networks.
- Category 3 – Unaccompanied youth or families with children/youth who meet the homeless definition under another federal statute.
- Category 4 – Individuals/families fleeing or attempting to flee domestic violence.
    - Any individual/family who:
        - (i) Is fleeing, or is attempting to flee, domestic violence, dating violence, sexual assault, stalking, human trafficking, or other dangerous or life-threatening conditions that relate to violence against the individual or a family member, including a child, that has either taken place within the individual's or family's primary nighttime residence or has made the individual or family afraid to return to their primary nighttime residence;
        - (ii) Has no other residence; and
        - (iii) Lacks the resources or support networks, e.g., family, friends, and faith-based or other social networks, to obtain other permanent housing.

Homeless Emergency Aid Program (HEAP): A one-time $500 million block grant program created in 2018. HEAP was established to provide direct assistance to California's homeless Continuums of Care (CoCs) and large cities to address the homelessness crisis throughout the state.

Homeless Housing, Assistance, and Prevention (HHAP): Signed into law on July 31, 2019, by Governor Gavin Newsom. The Homeless Housing, Assistance, and Prevention is a $650 million one-time block grant that provides local jurisdictions with funds to support regional coordination and expand or develop local capacity to address their immediate homelessness challenges.

Homeless Management Information System (HMIS): A local information technology system used to collect data on the provision of housing and services to homeless individuals/families.

Homelessness Prevention: A program targeted at individuals and families at risk of homelessness. Specifically, this includes those that meet the criteria under the "at risk of homelessness" definition at 24 CFR 576.2, as well as those who meet the criteria in Category 2, 3, and 4 of the "homeless" definition and have an annual income below 30% of family median income for the area.

Housing First: An approach to quickly and successfully connect individuals and families experiencing homelessness to permanent housing without preconditions and barriers to entry, such as sobriety, treatment, or service participation requirements. Supportive services are offered to maximize housing stability and prevent returns to homelessness instead of addressing predetermined treatment goals before permanent housing entry.

Housing Interventions: Housing programs and subsidies, including transitional housing, rapid re-housing, permanent supportive housing programs, and permanent housing subsidy programs (e.g., Housing Choice Vouchers).

Housing and Urban Development (HUD): The United States Department of Housing and Urban Development.

Literally Homeless: Category 1 of HUD's definition of homelessness. Literally Homeless means an individual or family who lacks a fixed, regular, and adequate nighttime residence, meaning the individual or family has a primary nighttime residence that is a public or private place not meant for human habitation, the individual or family is living in a publicly or privately operated shelter designated to provide temporary living arrangements (including hotels and motels paid for by charitable organizations or federal, state, or local government programs), or the individual is existing an institution where they have resided for 90 days or less and who lived in an emergency shelter or place not meant for human habitation immediately before entering that institution.

Master List: A prioritized list in HMIS of people who have completed the assessment survey and need permanent housing. The list can be sorted by essential eligibility criteria and is prioritized so that individuals and families with the greatest need are housed first.

Permanent Supportive Housing (PSH): A type of permanent housing designed for chronically homeless and other highly vulnerable individuals and families who need long-term support to stay housed. Permanent supportive housing provides housing linked with case management and other supportive services. Permanent supportive housing has no time limitation, providing support for as long as needed and desired by the resident.

Rapid Rehousing (RRH): A type of permanent housing program (PH) designed to provide short-term financial assistance and support to quickly re-house homeless households in independent housing. The goal is to promptly move households out of homelessness and back into permanent housing, providing the lightest level of service necessary to assist the household.

Release of Information (ROI): The consent form that individuals/households complete and sign to grant consent for their personal information to be entered into HMIS and used for coordinated entry.

Transitional Housing: Temporary housing with services to facilitate movement of homeless individuals and families to permanent housing within 24 months

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

Vulnerability Index: Service Prioritization Decision Assistance Tool (VI-SPDAT) – a pre-screening tool designed by OrgCode Consulting, Inc. and Community Solutions that can be conducted to quickly determine whether a client has high, moderate, or low acuity.

Attachment B: VAWA Considerations

Attachment C: Client Consent Levels

Client Data Categories	**Summary of Notification/Consent and Data Sharing Procedures**
Primary Identifiers: • Name and Aliases • Birth Date • Gender • Social Security Number • Family/Relationship Information	Open Client record: If the client does not ask to hide his/her identifiers, the primary identifiers will be available to all HMIS users in the Client Search to locate an existing client. None of the other client information will be viewable, except as described below. Closed Client record: If a client asks to hide his/her primary identifiers, the record will appear on the Client Search List only for the originating agency. It will be hidden from all other agencies. Some system-level users will have access to hidden records for system administration purposes.
General Client Information (Demographics, Entry/Exit, and Service Transactions): • Ethnicity • Race • Services Provided • Program Enrollment (Entry/Exit)	Open Assessment: With a signed release of information (ROI), these data can be shared with HMIS users from partner agencies by opening/unlocking the Demographics assessment and relevant Entry/Exit and Service Transactions. Closed Assessment: If written consent is not provided, this information is accessible only within the originating agency and some system-level users for system administration purposes.
Protected Information: • Housing History • Income/Benefits/Employment • Disability information • Mental Health Assessment • Substance Abuse Assessment • HIV/AIDS Information • Domestic Violence Information • Veteran status and information	Protected Information: Generally, this information is available only within the originating agency to users that have an authorized access level and to authorized system-level users for system administration purposes. Any other sharing of this data should be limited to specific Partner Agencies as a closed exception and require signed consent from the client.