December 11, 2014
Contra Costa County
Homeless Management Information System

CoC-HMIS Governance Charter, Policies & Procedures

Contra Costa HMIS Project Staff
1350 Arnold Drive, Suite 202
Martinez, CA 94553

Revision History

Date	Author	Description
03/21/2006	Evan Smith	Changes to reflect edits made at the 02/2006 COCB HMIS Meeting
04/21/2006	Evan Smith	Changes to reflect edits made at the 03/2006 COCB HMIS Meeting
05/22/2006	Evan Smith	Changes to reflect edits made at the 04/2006 COCB HMIS Meeting
06/4/2009	Kim Baello	Added “24 hours or 1 business day” under 5.3 Policies
12/11/2014	HMIS Policy Committee	Changes to reflect edits made at 02 – 09/2014 HMIS Policy Committee meetings

TABLE OF CONTENTS

1. Introduction

This document provides the framework for the ongoing operations of the Contra Costa County Homeless Management Information System (CONTRA COSTA HMIS) Project. The Project Overview provides the main objectives, direction and benefits of the CONTRA COSTA HMIS Project. Governing Principles establish the values that are the basis for all policy statements and subsequent decisions. This document also serves as the Governance Charter, establishing the relationship between the Contra Costa County Continuum of Care (the Continuum, CoC, or CCICH) and Contra Costa County Behavioral Health Homeless Program (HP) (the Collaborative Applicant and HMIS Lead Agency).

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 external relationships required for the continuation of this project. Forms Control provides information on obtaining forms, filing and record keeping.

2. 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 Continuum in a better position to request funding from various sources and help plan better for future needs.

The mission of the Homeless Management Information System of the Contra Costa County Continuum of Care is to be an integrated network of homeless and other service providers that use a central database to collect, track and report uniform information on client needs and services. This system will not only meet Federal requirements but also enhance service planning and delivery.

The fundamental goal of the CONTRA COSTA HMIS Project is to document the demographics of homelessness in Contra Costa County according to the HUD HMIS Standards. It is then the goal of the project to identify patterns in the utilization of assistance, and document the effectiveness of the services for the client. This will be accomplished through analysis of data that is gathered from the actual experiences of homeless persons and the service providers who assist them in shelters and homeless assistance programs throughout the county. Data that is gathered via intake interviews and program participation will be used to complete HUD Annual Progress Reports. This data may also be analyzed to provide unduplicated counts and anonymous aggregate data to policy makers, service providers, advocates, and consumer representatives.

The project utilizes a web-enabled application residing on a central server to facilitate data collection by homeless service organizations across the county. Access to the central server is limited to agencies formally participating in the project and then only to authorized staff members that meet the necessary training and security requirements.

The CONTRA COSTA HMIS Project is staffed and advised by Contra Costa County Behavioral Health Homeless Program. HP's Executive Director is the authorizing agent for all agreements made between Partner Agencies and HP. Bowman Systems is responsible for the administration of the central server

and system administration. COHP Project Staff will also provide technology, training and technical assistance to users of the system throughout the county.

The HMIS Policy Committee of Contra Costa County Continuum of Care (The Continuum) is responsible for oversight and guidance of The CONTRA COSTA HMIS Project. This group is committed to balancing the interests and needs of all stakeholders involved: homeless men, women, and children; service providers; and policy makers.

Potential benefits for homeless men, women, and children and case managers: Service coordination can be improved when information is shared among case management staff within one agency or with staff in other agencies (with written client consent) who are serving the same clients.

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

Potential benefits for community-wide Continuums of Care and policy makers: County-wide involvement in the project provides the capacity to generate HUD Annual Progress Reports for the CoC and allows access to aggregate information both at the local and regional level that will assist in identification of gaps in services, as well as the completion of other service reports used to inform policy decisions aimed at addressing and ending homelessness at local, state and federal levels.

3. Governing Principles

Described below are the overall governing principles upon which all other decisions pertaining to the CONTRA COSTA HMIS Project are based.

Participants are expected to read, understand, and adhere to the spirit of these principles, even when the 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, which are the primary focus of agency programs participating in this project.

Policies regarding client data will be founded on the premise that a client owns his/her own personal information and will provide the necessary safeguards to protect client, agency, and policy level interests. Collection, access and disclosure of client data through HMIS will only be permitted by the procedures set forth in this document.

Data Integrity

Client data is the most valuable and sensitive asset of the CONTRA COSTA HMIS Project. These policies will ensure integrity 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 countywide aggregation of unduplicated homeless statistics. The System Administrator is responsible for ensuring the broadest deployment and availability for homeless service agencies in Contra Costa County.

Compliance

Violation of the policies and procedures set forth in this document will have serious consequences. Any deliberate or unintentional action resulting in a breach of confidentiality or loss of data integrity will result in the withdrawal of system access for the offending entity.

Policies

- Compliance with these Policies and Procedures is mandatory for participation in the CONTRA COSTA HMIS system.
- Using the ServicePoint software, all changes to client data are recorded and will be periodically and randomly audited for compliance.

Procedures

- See Project Participation and User Authorization sections for procedures to be taken for lack of compliance.

4. Roles and Responsibilities

Contra Costa County Continuum of Care (The Continuum)

- **Guardianship of Client Data**: The Continuum is responsible for holding in trust all data entered into the HMIS on behalf of the clients served by the community. It is responsible for ensuring that appropriate policies, procedures, and standards are in place governing the access, use, and dissemination of data stored in the system. It is the responsibility of the CoC to ensure that all records containing protected identifying information of any individual or family who applies for and/or receives CoC assistance will be kept secure and confidential.
- **HMIS Lead Agency**: The CoC is responsible for the selection of the HMIS Lead. HP has been designated as the HMIS Lead to operate and maintain the Contra Costa HMIS.

HMIS Policy Committee

- **HMIS Policy Making**: The HMIS Policy Committee of CCICH is responsible for drafting, reviewing, and approving all policies and procedures related to the operation of the HMIS as required by federal regulation, including but not limited to HMIS Policies & Procedures, Partner Agency Memorandum of Understanding, Privacy Plan, Security Plan, and Data Quality Plan.
- **Annual Review of this Governance Charter, Policies & Procedures**: The HMIS Policy Committee is responsible for reviewing HMIS policies and procedures in consultation with the Collaborative Applicant (HP), and updating this Governance Charter as necessary to comply with Section 578.7(b) of the McKinney-Vento Act.
- **HMIS Oversight:** The HMIS Policy Committee shall provide project direction and guidance, ensuring that HMIS is administered in compliance with HUD requirements. In addition, the HMIS Policy Committee is responsible for:
  - Technology Plan
  - Selection of system software
  - Approval of project forms and documentation
  - Project participation and feedback
  - Project Funding

Contra Costa County Behavioral Health Homeless Program (HP)

Duties and Responsibilities of HP as HMIS Lead Agency

- **Enforcement of Privacy, Security & Data Quality Plans**: This agreement incorporates by reference, and the Agency agrees to be bound by, written HMIS policies and procedures for privacy, security and data quality as to be determined by the CoC. These policies will be drafted and updated as required to ensure compliance with HUD HMIS Notices on HMIS Governance, Privacy and Security, Software Functionality, and Data Quality upon release of the HMIS Requirements Final Rule when it becomes effective.
- **Security**: In addition to any duties and responsibilities included in the HMIS Security Plan, the Agency shall be responsible for making all reasonable efforts to maintain and secure client records, HMIS, and supporting services.
    - **User Credentials**: The Agency shall assign and maintain user identification and passwords for all HMIS users and monitor and log use of anyone accessing client data.
    - **Network Security**: The Agency shall take all reasonable efforts to ensure the security and integrity of the client database, including implementation and maintenance of appropriate firewalls, intrusion prevention systems (IPS), and other security measures as required in order to ensure the integrity of HMIS, including mobile security measures. The Agency shall conduct regular audits of HMIS security and report any significant vulnerabilities to the CoC.
- **Data Quality**: In addition to any duties and responsibilities included in the HMIS Data Quality Plan, the Agency will be responsible for making all reasonable efforts to ensure the highest level of data quality possible.
    - **Universal Data Elements**: The Agency shall ensure the HMIS is capable of managing the collection of each data variable and corresponding response category for each of the Universal Data Elements outlined in the HUD HMIS data and Technical Standards.
    - **Program-Specific Data Elements**: The Agency shall ensure the HMIS is capable of managing the collection of each data variable and corresponding response category for each of the Program-specific data elements as outlined in the HMIS Data and Technical Standards.
    - **Unduplicated Client Records**: The Agency shall ensure HMIS is capable of generating a summary of the number of unduplicated client records entered into HMIS.
    - **Program Entry and Exit Dates**: The Agency shall be responsible for ensuring the accurate entry of program entry and exit dates. Program entry and exit dates should be recorded 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 the last day a service was provided.
- **End User Training & Support**: The Agency shall be responsible for providing initial and on-going HMIS training, support and technical assistance to all participating agencies that use HMIS. The Agency shall work with participating agencies serving homeless clients and assist them with the process of entering information into HMIS, and shall strive for real-time, or close to real-time data entry.
- **Software Updates, Patches & Maintenance**: The Agency shall be responsible for ensuring all software and supporting services are updated, patched and otherwise maintained to the extent required in order to fulfill the agency's obligations under this agreement. The Agency shall serve as liaison to Bowman Systems on behalf of the CoC and partner agencies.
- **Other Federal Requirements**
    - **Drug-Free Workplace***:* The HMIS Lead Agency shall adopt drug-free workplace policy in compliance with the requirements of the Drug-Free Workplace Act. This policy must be published and distributed to employees, notifying them that the unlawful manufacture, distribution, dispensing, possession or use of a controlled

substance is prohibited and specifying actions that shall be taken against employees for violation of such a prohibition.
    - **Homeless Client Participation***:* In determining HMIS policy, the CoC Board or designated body shall include at least one homeless person or formerly homeless person in policymaking decisions. Participation can include but is not limited to governing board leadership, advisory committees, staff positions, and sub-committee positions.
    - **Equal Opportunity and Non-Discrimination***:* The HMIS Lead Agency adopts an equal opportunity and non-discrimination policy in compliance with Title VI of the Civil Rights Act of 1964, Section 504 of the Rehabilitation Act of 1973, the Age Discrimination Act of 1975, and HUD regulations.

HP Executive Director

- Liaison with HUD
- Project Staffing
- HP signatory for Memoranda of Understandings
- Overall responsibility for success of the CONTRA COSTA HMIS project

Project Manager / System Administrator

- Procurement of server software and licenses
- Post current HMIS documents on County Website
- Project Policies & Procedures and compliance
- General responsibility for project rollout
- Keeper of signed Memorandums of Understanding and User Agreements
- User Administration
- System Uptime & Performance Monitoring
- Ongoing Protection of Confidential Data
- Curriculum Development & Trainings
- Outreach/End User Support
- Adherence to Contra Costa County & HUD Data Standards
- 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 within constraints of other duties)

Partner Agency (PA)

For full details of Partner Agency duties and responsibilities, see the Memorandum of Understanding (MOU) Between Contra Costa County Behavioral Health Homeless Program and Partner Agency and the Partner Agency User Agreement and Technical User Agreement. The MOU and User Agreements are reviewed annually and updated as needed by the Policy Committee.

PA Executive Director

- Authorizing agent for partner agreement (MOU)
- Designation of HMIS Technical Administrator
- Agency compliance with Policies & Procedures
- End user licenses
- Agency level HUD reporting

Partner Agency HMIS Technical Administrator

- Authorizing agent for Partner Agency User Agreements
- Keeper of Partner Agency User Agreements
- Keeper of executed Client Informed Consent forms
- Authorizing agent for user ID requests

- Staff workstations
- Internet connectivity
- End user adherence to workstation security policies
- Detecting and responding to violations of the Policies and Procedures
- First level End user support
- Maintain Agency/Program Data in HMIS Application
- Authorized imports of client data

Agency Staff

- Safeguard Client Privacy through Compliance with confidentiality policies
- Data Collection as specified by training and other documentation.

Homeless Program Director

The Contra Costa County Homeless Director will serve as the Program Director for CONTRA COSTA HMIS participants. While every participant in the system, including clients, should have access to the Program Director, reasonable efforts should be made (and documented if possible) to obtain resolution by other means, including escalation within an agency and through HP.

The current Program Director may be contacted as follows:

Lavonna Martin
Acting Director, Homeless Program
Lavonna.Martin@hsd.cccounty.us

5. USE OF HMIS COMPONENT GRANT FUNDS

The HMIS Lead Agency is the only entity eligible to use grant funds for an HMIS component, and funded activities must comply with HUD HMIS requirements. The Agency has the following specific reporting requirements:

- **Annual Performance Reports**: The Agency shall ensure the HMIS is capable of generating a consistently reliable Annual Performance Report (APR) in compliance with the latest HUD guidance.

- **Annual Homeless Assessment Reports**: The Agency shall prepare and submit Annual Homeless Assessment Reports (AHAR) to HUD.

- **CoC Competition Community Application**: The Agency shall provide all necessary support required for the CoC to fully and accurately complete the community application portion of the HUD McKinney-Vento Continuum of Care competition.

- **High-Performing Communities Application**: The Agency shall at the CoC's request provide all necessary data and support required to support the collaborative applicant's application for designation as a High Performing Community under Section 424 of the McKinney-Vento Act.

6. OPERATING PROCEDURES

6.1 Project Participation

Policies

- Agencies participating in the CONTRA COSTA HMIS Project shall commit to abide by the governing principles of the CONTRA COSTA HMIS Project and adhere to the terms and conditions of this partnership as detailed in the Memorandum of Understanding.
- The Partner Agency shall pay a participation fee charged by the HMIS Lead Agency as specified in the fee schedule addendum to the Memorandum of Understand.

Procedures

Confirm Participation

1. The Partner Agency shall confirm their participation in the CONTRA COSTA HMIS Project by submitting a Memorandum of Understanding to the HP System Administrator.
2. The Project Manager will obtain the co-signature of HP Program Director.
3. The Project Manager will maintain a file of all signed Memorandums of Understanding
4. The HP System Administrator will update the list of all Partner Agencies and make it available to the project community and post this list on the HMIS website (http://cchealth.org/homeless/hmis.php/).
5. All participating Agencies will be listed on the CONTRA COSTA HMIS website.

Terminate Participation

Voluntary

1. The Partner Agency shall inform the HP System Administrator in writing of its intention to terminate its agreement to participate in CONTRA COSTA HMIS Project.
2. The HP System Administrator will provide a 30 Day Notice and inform the HP Executive Director and update the Participating Agency List.
3. The HP System Administrator will revoke access of the Partner Agency staff to the CONTRA COSTA HMIS. Note: All Partner Agency-specific information contained in the HMIS system will remain in the HMIS system upon termination.
4. The HP System Administrator will keep all termination records on file with the associated Memorandums of Understanding.

Lack of Compliance

1. When the HP System Administrator determines that a Partner Agency is in violation of the terms of the partnership, Executive Directors of Partner Agency and HP will work to resolve the conflict(s).
2. If Executive Directors are unable to resolve conflict(s), the HP Program Director will be called upon to resolve the conflict. If that results in a ruling of Termination:
    i. The Partner Agency will be notified in writing of the intention to terminate their participation in the CONTRA COSTA HMIS Project.
    ii. The HP System Administrator will revoke access of the Partner Agency staff to the CONTRA COSTA HMIS.
    iii. The HP System Administrator will keep all termination records on file with the associated Memorandums of Understanding.

List of primary contacts for each agency

1. The Partner Agency shall designate a primary contact for communications regarding CONTRA COSTA HMIS by submitting a Partner Agency Technical Administrator Agreement form to the HP System Administrator.
2. The HP System Administrator will maintain a file of all signed Technical Administrator Assignment forms.
3. The HP System Administrator will maintain a list of all assigned Technical Administrators and make it available to the project staff.

Re-Assign Technical Administrator

1. The Partner Agency may designate a new or replacement primary contact in the same manner as above.

Site Security Assessment

1. Prior to allowing access to the HMIS, the Partner Agency Technical Administrator and the HP System Administrator will meet to review and assess the security measures in place to protect client data. Meeting of Agency Executive Director (or designee), Program Manager/Administrator and Agency Technology Administrator with HP staff member to assess agency information security protocols. This review shall in no way reduce the responsibility for agency information security, which is the full and complete responsibility of the agency, its Executive Director, and Technical Administrator.
2. Agencies shall have the latest version of virus protection software on all computers that access HMIS.

6.2 User Authorization & Passwords

Policies

- Agency Staff participating in the CONTRA COSTA HMIS Project shall commit to abide by the governing principles of the CONTRA COSTA HMIS Project and adhere to the terms and conditions of the Partner Agency User Agreement.
- The Partner Agency Technical 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 must never use or allow use of a user ID that is not assigned to them. [See User Agreement]
- Temporary, first time only, passwords will be communicated via email to the owner of the User ID.
- User specified passwords must never be shared and should never be communicated in any format.
- New User IDs must require password change on first use.
- Passwords must consist of at least 8 characters and must contain a combination of letters and numbers (no special characters; alpha and numeric only). The password must contain at least two numbers [required by software].
    - According to the HUD Data and Technical Standards Final Notice (July 2004): “User authentication. Baseline Requirement. A CHO must secure HMIS systems with, at a minimum, a user authentication system consisting of a username and password. Passwords must be at least eight characters long and meet reasonable industry standard requirements.”

- Passwords must be changed every 45 days. If they are not changed within that time period, they will expire and the user will be locked out of the system.
- Three consecutive unsuccessful attempts to login will disable the User ID until the account is reactivated by a Partner Agency Technical Administrator or the CONTRA COSTA HMIS Administrator.

Procedures

Workstation Security Assessment

1. Prior to requesting user access for any staff member, the Partner Agency Technical Administrator will assess the operational security of the user's workspace.
2. Partner Agency Technical Administrator will confirm that workstation has up to date virus protection properly installed and that a full-system scan has been performed within the last week.

Request New User ID

1. When the Partner Agency Technical Administrator identifies a staff member that requires access to CONTRA COSTA HMIS, a *Partner Agency User Agreement (PAUA*) will be provided to the prospective User.
2. The Prospective User must read, understand and sign the *PAUA* and return it to the Partner Agency Technical Administrator.
3. The Partner Agency Technical Administrator will co-sign the *PAUA* and keep it on file.
4. The Partner Agency Technical Administrator will create the new user ID as specified and notify the user ID owner of the temporary password via email.

Change User Access

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

Rescind User Access

Voluntary: Use this procedure when any HMIS user leaves the agency or otherwise becomes inactive.

Compliance Failure: Use this procedure when any HMIS user breaches the User Agreement, or violates the Policies & Procedures, or breaches confidentiality or security.

1. The PA Technical Admin will deactivate staff User IDs
2. The HP System Administrator will deactivate all other User IDs.

Reset Password

1. When a user forgets their password or has reason to believe that someone else has gained access to their password, they must immediately notify their Partner Agency Technical Administrator.
2. The PA Technical Administrator will reset the user's password and notify the user of their new temporary password.

6.3 Collection and Entry of Client Data

Policies

- Client Data will be gathered according to the policies, procedures and confidentiality rules meeting the minimum threshold of HUD data standards.
- Client Data may only be entered into the HMIS with client's authorization to do so.
- Client Data will only be shared with Partner Agencies if the Client consents, has signed the Client Consent form, and the signed Client Consent form is available on record.
- Client Data will be entered into the HMIS in a timely manner in compliance with the guidelines set in the HMIS Data Quality Plan.
- All Client Data entered into the HMIS will be kept as accurate and as current as possible.
- Hardcopy or electronic files will continue to be maintained according to individual program requirements.
- No data may 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.

Procedures

- Refer to Policies & Procedures Materials and/or data entry guidelines.

6.4 Release and Disclosure of Client Data

Policies

- The HMIS Lead Agency shall ensure compliance with relevant federal and state confidentiality regulations and laws that protect client records. The Agency shall only release client records with the consent of the client, unless otherwise provided for by law.
- Substance Abuse Records: The Agency shall abide specially by federal confidentiality regulations as contained in the Code of Federal Regulations, 42 CFR Part 2 regarding disclosure of alcohol and/or drug abuse records unless disclosure is expressly permitted by informed written consent of the person whom it pertains to or as otherwise permitted by 42 CFR Part 2. A general authorization for the release of medical or other information is not sufficient for this purpose. The Agency understands that federal rules restrict use of the information to criminally investigate any alcohol or drug abuse patients.
- 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 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.
- Sharing of client data may be limited by program specific confidentiality rules.
- No client-specific data will be released or shared outside of the partner agencies unless the client gives specific written permission or unless withholding that information would be illegal. Please see Release of Information. Note that services may NOT be denied if client refuses to sign Release of Information or declines to state any information.
- Client Consent: Release of Information must constitute INFORMED consent. The burden rests with the intake counselor to inform the client before asking for consent.
- The Agency shall not require or imply that services must be contingent upon a Client's participation in HMIS. Services should be provided to a client regardless of HMIS participation, provided the client would otherwise be eligible for services.
- Client shall be given a print out of all data relating to them upon written request and within 10 working days.

- A report of data sharing events, including dates, agencies, persons, and other details, must be made available to the client upon written request and within 15 days or according to agency policy.
- A log of all external releases or disclosures must be maintained for seven (7) years and made available to the client upon written request and within 15 days or according to agency policy.
- Aggregate system wide 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 their agency's internal compliance with the HUD Data Standard.

Procedures

- Procedures for disclosure of client-specific data are readily obtained from the above policies, combined with the configuration of the CONTRA COSTA HMIS system, which facilitates appropriate data sharing.

6.5 Aggregate Data Access

Policies

- The Agency shall provide reports using aggregate data to the CoC upon request, or to other entities for funding or planning purposes pertaining to providing services to homeless persons, for homeless policy and planning decisions, in preparing federal, state or local applications for funding, to demonstrate the need for and effectiveness of programs, and to obtain a system-wide view of program utilization in the state.
- The Agency shall use only unidentified, aggregate data.

Procedures

- The Agency is responsible for ensuring that reporting access is maintained at the proscribed levels for agency clients, non-agency clients, and aggregate information reporting.

6.6 Proprietary Rights & Abuse

Policies

- **Copyright***:* The Contra Costa HMIS, underlying software, and services are protected by copyright and cannot be copied, except as permitted by law or written agreement with the copyright holder.
- **Unauthorized Access and Abuse***:* The HMIS Lead Agency shall take reasonable efforts to prevent the unauthorized access, use or modification of HMIS, or interference with normal system operation. This shall include both corruption of the HMIS database in any manner, as well as unauthorized disclosure or sharing of user identification and/or passwords. The Agency shall not use HMIS with intent to defraud federal, state or local governments, individuals or entities, or to conduct any illegal activity.

Procedures

- The HMIS Lead Agency shall be responsible for monitoring and preventing unauthorized access, use, or modification of HMIS, or interference with normal system operation.

6.7 Workstation Security

Policies

- Partner Agency Technical Administrator is responsible for preventing degradation of the whole system resulting from viruses, intrusion, or other factors under the agency's control.
- Partner Agency Technical Administrator or their delegate is responsible for preventing inadvertent release of confidential client-specific information. Such release may come from physical or electronic or even visual access to the workstation, 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).
- Definition and communication of all procedures to all Agency users for achieving proper agency workstation configuration and for protecting their access by all Agency users to the wider system are the responsibility of the Partner Agency Technical Administrator.
- Additional security policies are included in the Security Plan.

Procedures

- At a minimum, any workstation accessing the HMIS System shall have anti-virus software with current virus definitions (24 hours) and frequent full-system scans (weekly).

6.8 Training

Policies

- Agency Executive Director shall direct the Agency Technical Administrator and designated staff persons to attend training(s) as specified in the *Memorandum of Understanding* (MOU) between Partner Agency and HP.

Procedures

Training

HP will provide training in the following areas prior to Partner Agency using CONTRA COSTA HMIS:

- Agency Technical Administrator Training
- End User Training
- Confidentiality Training

Agency Technical 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:

- New user set-up
- Assigning Agency within CONTRA COSTA HMIS hierarchy.
- End user training
- Running package reports
- Creating customized reports

Ongoing Training

HP will provide regular training for the Continuum of Care, as needed. The areas covered will be:

- Agency Technical Administrator Training
- End User Training
- Confidentiality Training

6.9 Technical Support

Policies

- Support Requests include problem reporting, requests for enhancements (features), or other general technical support.
- Users shall submit support requests to their Partner Agency Technical Administrator (email is suggested).
- Users shall not submit requests to software vendor.
- Users shall not submit requests directly to HP without specific invitation. All requests to HP shall be submitted to Partner Agency Technical Administrator, who may then escalate to HP, who may then escalate to vendors as appropriate.
- HP will only provide support for issues specific to the CONTRA COSTA HMIS software and systems.

Procedures

Submission of Support Request

1. User encounters problem or originates idea for improvement to system or software.
2. End User creates Support Request to Partner Agency Technical Administrator.
3. Partner Agency Technical Administrator, upon receipt of a Support Request, shall make reasonable attempts to resolve the issue.
4. If the Partner Agency Technical Administrator is unable to resolve the issue and determines that the problem is specific to CONTRA COSTA HMIS software and systems contact the HMIS systems administrator.
5. System Administrator will consolidate such requests from multiple Partner Agencies, if appropriate, and strive to resolve issues in priority order according to their severity and impact.
6. If the System Administrator is unable to resolve the issue, other software or system vendor(s) may be included in order to resolve the issue(s).
7. In cases where issue resolution may be achieved by the end user or other Partner Agency personnel, System Administrator will provide instructions via email to Partner Agency Technical Administrator.

6.10 Changes to this and other Documents

Policies

- The HMIS Policy Committee of The Continuum will guide the compilation and amendment of these Policies and Procedures. The HMIS Policy Committee will review this document on a annual basis.

Procedures

Changes to Policies & Procedures

1. Proposed changes may originate from any participant in the CONTRA COSTA HMIS.
2. When proposed changes originate within a Partner Agency, they must be reviewed by the HMIS Policy Committee.
3. CONTRA COSTA HMIS System Administrator will maintain a list of proposed changes.
4. The list of proposed changes will be discussed by the Policy Committee, subject to line item excision and modification. This discussion may occur either at a meeting of the Technology Committee, or via email or conference call, according to the discretion and direction of the Technology Committee Chairperson.

5. Results of said discussion will be communicated, along with the amended Policies and Procedures. The revised Policies and Procedures will be identified within the document by the date of the Policy Committee discussion.
6. Partner Agencies Executive Directors shall acknowledge receipt and acceptance of the revised Policies and Procedures within 10 working days of delivery of the amended Policies and Procedures by notification in writing or email to System Administrator. P.A. Technical Administrator (cc to E.D.) shall also ensure circulation of the revised document within their agency and compliance with the revised Policies and Procedures.

7. Forms Control

All forms required by these procedures are available in pdf format on the Homeless Program website, located at http://cchealth.org/homeless/data-evaluation/.

HMIS DATA SECURITY PLAN

Overview

HUD regulations require that Continuums of Care establish HMIS Data Security Plans. This Data Security Plan is based upon the HMIS Requirements Proposed Rule released in December 2011, and may be edited upon the release of further guidance by HUD.

Applicability

CONTRA COSTA HMIS participating agencies must apply system security provisions to all the systems where personal protected information (PPI) is stored, including, but not limited to, its networks, desktops, laptops, tablets, phones, mainframes and servers.

User Authentication

Upon successful completion of training and submission of signed User Agreement to the HMIS Lead, each HMIS user will be provided with a unique personal User Identification Code (User ID) and initial password to access the HMIS. While the User ID provided will not change, HUD standards require that the initial password only be valid for the user's first access to the HMIS. Upon access with the initial password, the user will see a screen that will prompt the user to change the initial password to a personal password created by the user. The Partner Agency Technical Administrator must only request user access to HMIS for those staff members that require access to perform their job duties.

The password created by the user must meet the following Federal and application-enforced guidelines from the CoC-HMIS Governance Charter Policies and Procedures:

a. All users must have their own unique user ID and must never use or allow use of a user ID that is not assigned to them. (See User Agreement.)
b. Temporary, first time only, passwords will be communicated via email to the owner of the User ID.
c. User specified passwords must never be shared and should never be communicated in any format.
d. New User IDs must require password change on first use. Passwords must contain of at least 8 characters and must contain a combination of letters and numbers. The password must contain at least two numbers or symbols (required by software). (Refer to the HUD Data and Technical Standards Final Notice (July 2004) for additional guidance.)

Agencies participating in the CONTRA COSTA HMIS shall commit to abide by the governing principles of the CONTRA COSTA HMIS Project and shall adhere to the terms and conditions of this partnership as detailed in the Memorandum of Understanding attached.

Agencies participating in the CONTRA COSTA HMIS shall commit to abide by the

governing principles in the CoC-HMIS Governance Charter, Policies & Procedures.

Prior to allowing access to the HMIS, the Partner Agency Technical Administrator will agree to review and assess the security measures in place to protect client data. A Homeless Program staff member will meet Agency Executive Director (or designee), Program Manager / Administrator and Agency Technology Administrator to access agency information security protocols. This review shall in no way reduce the responsibility for agency information security, which is the full and complete responsibility of the agency, its Executive Director, and Technical Administrator.

Security Training

The HMIS Lead will ensure that all users receive security training prior to being given access to the HMIS, and that the training curriculum reflects the CoC-HMIS Governance Charter, Policies & Procedures and HUD requirements. HMIS security training will be offered at least annually.

Application Security

Agencies must ensure that all computers connecting to HMIS run a current version of anti-virus software. This is enforced through an Active Directory network policy, and applies to both devices directly attached to an area-wide network as well as those at service provider locations that connect through the public Internet via a Secure Socket Layer (SSL) Virtual Private Network (VPN) tunnel connection. Individual computers are scanned and only allowed to connect to the network when the presence of updated anti/virus software from an approved list has been verified. This appliance also provides protection against phishing, malware; bot attacks and provides access control to limit users to appropriate resources.

HMIS Participating Agencies must maintain anti-virus software on all devices on their network. Devices that access the Internet must be configured to automatically download updated virus definitions. Steps should also be taken to prevent the intrusion of “adware” and “spyware” programs.

The Agency Technical Administrator maintains hardware, software and PPI in a secure environment, protected by a Firewall. Users must take appropriate steps to ensure that networks used outside of the agency are secured in compliance with this section.

Physical Control over Devices With Access to HMIS Data

HMIS Participating Agencies must staff devices at all times that are stationed in public areas and used to collect HMIS data. Every device that is used to access the HMIS must have a password-protected screen saver that automatically turns on when the device is temporarily not in use. If an HMIS user will be away from the device for an extended period of time, he or she is required to log off from HMIS before leaving the work area in which the device is located.

Disaster Protection and Recovery

HMIS is contained on SQL 2005 databases which are run on a Windows Server clustered environment so that there will be failover protection if the primary server becomes unavailable. The physical data storage is on multiple disc drives in a RAID array for redundancy so that no data will be lost or downtime incurred if a physical disk drive becomes inoperable. Additional hardware redundancy exists in the form of dual power supplies, disc controllers and network interface cards. The HMIS Lead maintains service coverage through original and extended warranties from the original equipment manufacturer and assures that the systems are kept up to date in terms of patches and updates issued by both the software and hardware vendors. The SQL databases are automatically backed up nightly and stored on another secure server.

Bowman Systems is responsible for the disaster protection and recovery of the central server, as well as data disposal.

System Monitoring

HMIS produces reports based on log files that are reviewed and inactive user accounts are consequently disabled (e.g., in the event of a user leaving an agency, a job position change, etc.). In addition to the HMIS database itself, access to HMIS is also controlled, monitored and logged by Agency Technical Administrator.

Hard Copy Security

The guidelines regarding the security of paper or other hard copy containing PPI that is either generated by or for the HMIS, including, but not limited to reports, data entry forms, and signed consent forms are:

1. HMIS Participating Agency staff must supervise at all times any paper or other hard copy generated by or for the HMIS that contains PPI when the hard copy is in a public area.
2. When HMIS Participating Agency staff is not present, the information must be secured in areas that are not publically accessible.
3. Written information specifically pertaining to user access (e.g., User ID and password) must not be stored or displayed in any publicly accessible location.

HMIS DATA QUALITY PLAN

Overview

HUD regulations require Continuums of Care to establish HMIS Data Quality Plans. This Data Quality Plan is based upon the HMIS Requirements Proposed Rule released in December 2011, and may be edited upon the release of further guidance by HUD.

Timeliness

An HMIS should have the most current client information available for every person being actively served by service providers. All HMIS participants should strive to minimize the gap between when information is collected and when it is entered into HMIS, with the goal of real-time data entry whenever feasible. To that end, relevant client information should always be entered into HMIS within the following initial guidelines, based on project type:

- Emergency Shelter, Transitional Housing, Permanent Housing, Rapid Rehousing, and Prevention projects: All Universal and Program-Specific Data Elements entered within two (2) business days of intake.
- Outreach projects and Non-residential Support Service Only projects (SSO): Limited data elements entered within five (5) business days of the first outreach encounter. Upon engagement for services, all remaining Universal and Program-Specific Data Elements entered within two (2) business days.

Agencies with projects providing services should strive to meet these timeliness goals:

- All users must have their own unique user ID and must never use or allow use of a user ID that is not assigned to them. [See User Agreement.] User specified passwords must never be shared and should never be communicated in any format. Client identification and supplemental assessments should be entered within two (2) business days.
- Updates and interim reviews should be entered within two (2) business days of discovery of the event change.
- All service data should be entered within five (5) business days of service provision.

As data entry policies and procedures are developed and refined within each participating agency, the CoC shall review these timeliness guidelines and modify them accordingly. It is the goal of Contra Costa continuum of care to enter data into HMIS in the most timely manner feasible.

Completeness

Complete HMIS data is necessary to fully understand the demographic characteristics and service use of persons in the system. Complete data facilitates confident reporting and analysis on the nature and extent of homelessness, such as:

- Unduplicated counts of clients served at the local level;
- Patterns of use of people entering and exiting the homeless assistance system;

and

- Evaluation of the effectiveness of homeless systems.

In effect, complete data tells the full "story" of homelessness to the agencies, the Continuum, and the general public. To that end, all data entered into the HMIS shall be complete.

In addition, at the client level, more complete HMIS data improves quality of services and ability of provider staff to meet client needs, efficiently and effectively.

The Continuum's goal is to collect 100% of all data elements. However, the Continuum recognizes that this may not be possible in all cases. Therefore, the Continuum has established a data quality benchmark upper limit of 1% as an acceptable percent of null/missing and unknown/don't know/refused responses for all UDEs and program specific data elements excluding Domestic Violence and Social Security Number.

For exit dates, SSOs will close out these date if no contact has been made within 6 months.

Data completeness will be evaluated using an automated report generated by the HMIS that calculates the percent completes of required data elements. This figure will be considered when generating an overall data quality score, reflecting compliance with the Data Quality Plan.

Accuracy & Consistency

Accuracy of data in an HMIS can be difficult to assess because it depends on both the client's ability to provide the correct data and the intake worker's ability to document and enter the data accurately. Consistency directly affects the accuracy of data; if an end user collects all of the data, but they do not collect it in a consistent manner, then the data may not be accurate.

The purpose of accuracy is to ensure that the data in the CoC's HMIS is the best possible representation of reality as it relates to homeless people and the programs that serve them. To that end, all data entered into the CoC's HMIS shall be a reflection of information provided by the client, as documented by the intake worker or otherwise updated by the client and documented for reference. Recording inaccurate information is strictly prohibited.

All data in HMIS shall be collected and entered in a common and consistent manner across all programs. To that end, the CoC will undertake system-wide accuracy checks, require end user training, and maintain a consistent intake form.

- **Systemwide Checks**: HMIS Lead Agency staff will conduct periodic accuracy and consistency checks, including de-duplication efforts every 6 months, and will run automated searches for information that is likely inconsistent. Any data inconsistency issues identified by agency-level staff will be reported to the HMIS Administrator.

- **Data Accuracy Report**: Like the Data Completeness report, this report will be filed monthly. This report measures specific incongruency errors including but not limited to:
    - Client age/date of birth errors, multiple active incomes, and incongruences between housing status and living situation, chronic homelessness status and disability status, and income and employment status.

- **Client Enrollment Reports:** Like the Data Completeness and Data Accuracy reports, this report will be filed monthly. This report displays a list of new client intakes, exits, and active clients during the month. This report should be verified for accuracy prior to submission.

- **Training:** All intake and data entry workers will complete an initial training before accessing the live HMIS system, using the established train the trainer structure. Optional trainings will be offered annually to HMIS users wishing to recertify their knowledge of consistency practices.

- **Intake Form:** A basic intake form that collects data in a consistent manner will be available to all programs, which they can alter to meet their additional needs, provided the base document does not change. A document that outlines the basic data elements collected on the intake form, their response categories, rationale, and definitions will be made available in paper and via the HMIS website as a quick reference to ensure consistent data collection. New agencies that join the CoC are required to review this document as part of the HMIS Agency Agreement execution process.

Monitoring & Enforcement

The CoC recognizes that the data produced from the HMIS is critical to meet the reporting and compliance requirements of individual agencies and the CoC as a whole. As such, all HMIS agencies are expected to meet the data quality benchmarks described in this document. To achieve this, the HMIS data will be monitored periodically to quickly identify and resolve issues that affect the timeliness, completeness, and accuracy of the data. All monitoring will be done in accordance with the Data Quality Plan, with full support of the CoC membership. The timeframe to correct errors will be within 10 days following the end of the month unless the 10th of the month falls on a weekend, then which it will be the following Monday.

- Data Completeness and Data Accuracy Reports show a letter grade on the front page, corresponding to each agency's data completeness and data accuracy rate. These reports must be run on a monthly basis and submitted to the HMIS Lead Agency by the 10th of the following month. Once submitted, the HMIS System Administrator will evaluate and ensure that these reports meet the minimum-level required for compliance. All agencies are required to take the steps necessary to mitigate any errors and performance gaps prior to submission and must receive an "A" grade in both categories, reflecting compliance with this Data Quality Plan's benchmarks.

The purpose of monitoring is to ensure that the agreed-upon data quality benchmarks are met to the greatest possible extent and that data quality issues are quickly identified

and resolved. Monitoring will be considered in the annual CoC Program review & rank process. Participating agencies that are identified as needing assistance in addressing performance gaps will be offered refresher HMIS training courses and corrective plan technical assistance as needed.

HMIS CLIENT DATA & PRIVACY PLAN

Overview

HUD regulations require that Continuums of Care establish HMIS Data Privacy Plans after the HMIS Privacy and Security Notice is released. This Client Data & Privacy Plan is based upon the HMIS Requirements Proposed Rule released in December 2011, and may be edited upon the release of further guidance by HUD.

HMIS Data Sharing

Client-specific data from CONTRA COSTA HMIS may be shared with partner agencies only when the sharing agency has secured a valid Release of Information 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. HUD's HMIS Privacy and Security Notice may provide additional guidance on whether the Release of Information must have an expiration date.

Client Notification Policies and Procedures

HMIS Participating Agencies must let clients know that personal identifying information is being collected, and the reasons for collecting this information. To meet this requirement, HMIS Participating Agencies must (1) publicly post a Privacy Notice and (2) collect a Client Informed Consent & Release of Information (ROI) Authorization form.

- HMIS Participating Agencies must submit a copy of their Privacy Notice for the HMIS Administrator to keep on file. The Privacy Notice must, at a minimum, state that a copy of this Client Data & Privacy Plan is available upon request.
- CONTRA COSTA HMIS has prepared a standard document Client Informed Consent & Release of Information Authorization form. All written consent forms must be stored in a client's case management file for record-keeping and auditing purposes.

The Participating Agency shall uphold Federal and State Confidentiality regulations to protect client records and privacy. If an agency is covered by the Health Insurance Portability and Accountability Act (HIPAA), the HIPAA regulations prevail. The Agency shall not require or imply that services must be contingent upon a Client's participation in HMIS. Services should be provided to a client regardless of HMIS participation, provided the client would otherwise be eligible for services.

Data Purpose & Use Limitations

Each agency will use or disclose personal information for activities described in this part of the notice. The agency assumes that clients consent to the use or disclosure of personal information for the purposes described here and for other uses and disclosures that are determined to be compatible with these uses or disclosures:

a. To provide or coordinate services to individuals (shelter, housing, case management, etc.)
b. For functions related to payment or reimbursement for services

c. To carry out administrative functions such as personnel oversight, management functions, and auditing purposes
d. When required by law
e. To avert serious threat to health or safety if
    i. The agency believes that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public, and
    ii. The use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat
f. To report victims of abuse when authorized by law
g. For research purposes unless restricted by other federal and state laws.

Each agency shall only solicit or input into HMIS client information that is essential to providing services to the client. Each agency shall not knowingly enter false or misleading data under any circumstance, nor use HMIS with intent to defraud federal, state or local governments, individuals or entities, or to conduct any illegal activity.

Access and Correction

Each agency must allow individuals to inspect and have a copy of their personal information that is maintained in HMIS. Each agency must offer to explain any information that is not understood. Individuals must submit a request to inspect their HMIS data in writing to their social worker/case manager. Each agency must consider a written request for correction of inaccurate or incomplete, personal information. If the agency agrees that the information is inaccurate or incomplete, the agency may delete it may choose to mark it as inaccurate or incomplete and to supplement it with additional information.

Each agency may deny the individual's request for inspection or copying of personal information if:

a. Information was compiled in reasonable anticipation of litigation or comparable proceedings
b. Information is about another client/consumer
c. Information was obtained under a promise of confidentiality and the disclosure would reveal the source of the information, or
d. Disclosure of information would be reasonably likely to endanger the life or physical safety of any individual.

If the agency denies a request for access or correction, it must explain the reason for the denial and include documentation of the request and the reason for the denial. Each agency may reject repeated or harassing requests for access or correction.

Confidentiality

Each agency must maintain any/all personal information as required by federal, state, or local laws. Each agency shall ensure that all staff, volunteers and other persons who use HMIS are issued an individual User ID and password. Each agency shall ensure that all staff, volunteers and other persons issued a User ID and password for HMIS

receive confidentiality training, HMIS training, and comply with CONTRA COSTA HMIS Policies and Procedures.

Protections for Victims of Violence, Dating Violence, Sexual Assault, and Stalking

A Participating Agency may disclose PPI about an individual whom a it reasonably believes to be a victim of violence, dating violence, sexual assault, or stalking only to a government authority authorized by law to receive reports of abuse, neglect, or domestic violence where:

- Disclosure is required by law, and the disclosure complies with and is limited to the requirements of the law
- The individual agrees to the disclosure, or
- To the extent that the disclosure is expressly authorized by statute or regulation; and the Agency believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or if the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the PPI for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

A Participating Agency that makes a permitted disclosure about a must promptly inform the individual that a disclosure has been or will be made, except if 1) the Agency, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or 2) the Agency would be informing a personal representative (such as a family member or friend), and the Agency reasonably believes the personal representative is responsible for the abuse, neglect or other injury, and that informing the personal representative would not be in the best interests of the individual as determined by the Agency in the exercise of professional judgment.