CONTRA COSTA COUNTY CONTINUUM OF CARE

HOMELESS MANAGEMENT INFORMATION SYSTEM (HMIS)

HMIS GOVERNANCE CHARTER AND HMIS POLICIES & PROCEDURES

Adopted by Contra Costa Council on Homelessness – 05/06/2021

Contra Costa HMIS Project Staff
2400 Bisso Ln., Suite D2
Concord, CA 94520

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	Kimberly Thai, HMIS System Administrator	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
6/18/2018	Kimberly Thai, HMIS System Administrator	Name change for County Homeless division, Change of address for County Homeless division, Updated software vendor to Bitfocus Inc.
05/06/2021	HMIS Policy Committee	Changes to reflect edits approved by the HMIS Policy Committee during 04/2021 meeting
09/15/2022	Kimberly Thai, HMIS System Administrator	The CoC Data Quality Monitoring Plan has been formally approved and exists as a separate document. Removed from Appendix.
01/17/2024	Kimberly Thai, HMIS System Administrator	Updated Privacy Plan to include language around data breach notifications. Clarified language around how to store client release forms.
3/1/2024	Torrie Carlson, HMIS System Administrator	Updated https://cchealth.org/h3/coc/partners.php#HMIS to shortened URL: https://www.cchealth.org/hmis

TABLE OF CONTENTS

I. Overview

This document provides the framework for the ongoing operations of the Contra Costa County Homeless Management Information System (CONTRA COSTA HMIS). The document is organized into two main parts.

Part One contains the ***HMIS Governance Charter***, which outlines how HMIS will be managed and the responsible parties. The Governance Charter establishes the relationship between the Contra Costa County Continuum of Care (the Continuum or CoC) and Contra Costa County Health, Housing and Homeless Services division (H3) as both the Collaborative Applicant and the HMIS Lead Agency for the operation and oversight of HMIS.

Part Two consists of the ***HMIS Policies and Procedures***, which provide specific policies and steps necessary to control the operational environment and enforce compliance in the areas of:

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

A. Purpose of HMIS

The purpose and mission of the Homeless Management Information System of the Contra Costa County Continuum of Care is to serve as a central database to collect, track, analyze and report uniform client and activity data regarding the provision of shelter, housing, and services to individuals and families experiencing homelessness and at risk of homelessness within the Contra Costa CoC region.

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 improve planning efforts for future needs for the Contra Costa homeless system of care through evidence-based decision making.

A fundamental goal of CONTRA COSTA HMIS is to understand the trajectory of how clients are moving through the homeless system of care from access and enrollment to referral and housing. Data regarding clients' trajectory through the system can help identify patterns in utilization of services, effectiveness of services, and inform any gaps or process improvement points in the system. In addition, HMIS also documents the demographics of homelessness in Contra Costa County according to the U.S. Department of Housing and Urban Development (HUD) HMIS Standards. Demographic data is important in identifying the trends in the population of individuals and families experiencing homelessness to ensure individuals of different racial and ethnic backgrounds, age, gender, household size, and other subpopulations have access to and receive services within the CoC in a fair and equitable manner.

Data that is gathered in HMIS will be used to complete required local, state, and federal reporting requirements, including HUD Annual Progress Reports. HMIS data may also be analyzed to provide unduplicated counts and anonymous aggregate data to funders, policy makers, service providers, advocates, and clients and the public upon request.

HMIS 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 who meet the necessary training and security requirements.

B. HMIS Oversight & Support

The CONTRA COSTA HMIS is staffed and advised by the Contra Costa County Health, Housing, and Homeless Services division (H3), which acts as the HMIS Lead Agency. The HMIS System Administrator is the keeper for all agreements made between Partner Agencies and H3. Bitfocus, Inc. is responsible for the administration of the central server and administration of their software Clarity Human Services. H3 Staff will also provide technology, training and technical assistance to users of the system throughout the county.

The Contra Costa CoC Lead Agency, H3, is also responsible for oversight and direction of the CONTRA COSTA HMIS pursuant to the Contra Costa Council on Homelessness Governance Charter and HMIS Governance Charter.

The HMIS Policy Committee is responsible for oversight and guidance of the CONTRA COSTA HMIS. This group is committed to balancing the interests and needs of all stakeholders involved: individuals and households experiencing homelessness, including all children and adults; service providers; funders; policy makers, and system partners.

C. HMIS Benefits & Utility

Potential benefits for clients, service providers, and the system: Service coordination and delivery can be improved when information is shared among homeless service provider staff within one agency or with staff in other agencies (with client consent) who are serving the same clients.

Potential benefits for agencies and program managers: Aggregate 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 compliance and performance evaluations of agencies and program services, and/or report to funding agencies such as HUD and the State of California.

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

D. Key Terms

- **Client or Consumer**– person or persons experiencing or at-risk of homelessness that engage with the Contra Costa CoC to receive services.
- **Confidential Data** – data that includes personal identifying information (see below)
- **HMIS** – **Homeless Management Information System** - an internet-based database that is used by homeless service organizations across the Contra Costa CoC to record and store client-level information about the numbers, characteristics, needs, and service utilization of homeless persons and those at-risk of homelessness and must adhere to HUD Technical and Data Standards
- **Personally Identifiable Information (PII)** - data that identifies, either directly or indirectly, a specific individual; or can be manipulated by a reasonably foreseeable method to identify a specific individual; or can be linked with other available information to identify a specific individual
- **End User** – a Partner Agency staff member that is permitted to access and enter data into HMIS and must adhere to minimum training and security standards and the HMIS Policies and Procedures
- **HMIS Vendor** – the Contra Costa HMIS Vendor is Bitfocus, the entity that administers the central server of their HMIS software, Clarity Human Services
- **Minimum Data Entry Standards** – a minimum set of questions that must be completed for each client to provide data for use in aggregate analysis
- **HMIS Partner Agency (Partner Agency)** – a homeless service organization that uses HMIS in accordance with the Partner Agency HMIS MOU; the Partner Agency User Agreement and Partner Agency HMIS Administrator Agreement; and the HMIS Policies and Procedures herein
- **Partner Agency HMIS Agency Administrator (Agency Administrator or AA)** – staff at the Partner Agency responsible for serving as a liaison between the HMIS Lead and the Partner Agency. The Agency Administrator is responsible for providing first-tier technical support to End Users and ensuring that HMIS Policies and Procedures are complied with at the agency level.
- **Partner Agency HMIS MOU** - the Memorandum of Understanding Between Contra Costa County Health, Housing, and Homeless Services and a Partner Agency which includes the terms that the Partner Agency must adhere to maintain access and continue to be an active participant in HMIS
- **HMIS System Administrator** – staff at H3 who are responsible for overseeing HMIS users and ensuring compliance with the HMIS Policies and Procedures

II. Part One: HMIS Governance Charter

HMIS Governance Charter

A. Article 1: Purpose

The purpose of the HMIS Governance Charter (Governance Charter) is to establish the governance structure for the operation of Contra Costa HMIS. The Governance Charter articulates the decision-making process and formalizes the roles and responsibilities of the parties and entities involved in the management and operation of HMIS. Any roles and responsibilities identified in this Governance Charter are also subject to any Memorandum of Understanding documents between the either of the parties herein.

B. Article 2: Contra Costa Continuum of Care Responsibilities

The Contra Costa Continuum of Care is a community-based collaborative that oversees homeless system planning and coordination, including HMIS implementation in Contra Costa County. The Continuum includes community members, housing and services providers, a governing body (Council on Homelessness), and an administrative entity and staff (Contra Costa Health, Housing and Homeless Services Division (H3)). H3 acts as the CoC Lead Agency and Collaborative Applicant on behalf of the CoC. The Continuum has the following HMIS-related responsibilities:

HUD Responsibilities:

- **HMIS Lead Agency**: The CoC is responsible for the selection of the HMIS Lead.
- **Designating HMIS:** The CoC is responsible for designating a single information system as the official HMIS software for the geographic area.
- **Reviewing and Approving Policies and Plans**: The CoC is responsible for reviewing, revising, and approving an HMIS privacy plan, security plan, data quality plan, and other policies and plans required by federal regulation.
- **HMIS Participation**: The CoC is responsible for ensuring consistent participation of recipients and subrecipients in the HMIS.
- **HMIS Compliance**: The CoC is responsible for ensuring that the HMIS is administered in compliance with requirements prescribed by HUD.

In addition to the HUD-mandated responsibilities, the CoC Lead is responsible for conducting oversight and monitoring of the HMIS Lead to ensure compliance with HUD HMIS standards and alignment with local needs and CoC goals. For a full description of the roles and responsibilities of the CoC Lead Agency, refer to Section C.1 of the HMIS Policies and Procedures herein.

C. Article 3: Designations

HMIS Software

The CoC designates Clarity Human Services to serve as its HMIS. Clarity Human Services is a software product of Bitfocus, Inc., and will hereafter be referred to as the Clarity System.

HMIS Lead Agency

The CoC designates H3 as the HMIS Lead Agency for the Contra Costa HMIS.

D. Article 4: Responsibilities of the HMIS Lead

H3, as the HMIS Lead Agency, is responsible for the day-to-day management of HMIS, including monitoring Partner Agencies for compliance with HMIS policies and data quality, privacy, and security plans. The HMIS Lead Agency provides technical support and training to ensure compliance with local and federal policies and regulations. In addition, the HMIS Lead agency is responsible for authorizing/completing mandatory reporting to HUD. The HMIS Lead Agency develops plans, policies and procedures on behalf of the CoC, which are reviewed and approved by the CoC Lead, the HMIS Policy Committee, and the Council on Homelessness. For a full description of the roles and responsibilities of the HMIS Lead, refer to Section C.2 of the HMIS Policies and Procedures herein.

E. Article 5: Responsibilities of the HMIS Policy Committee

The HMIS Policy Committee of the CoC is responsible for reviewing and approving HMIS related policies, conducting an annual review of the HMIS Governance Charter in partnership with the HMIS Lead and the CoC Lead, and providing direction and guidance on HMIS policies on an ongoing basis. For a full description of the roles and responsibilities of the HMIS Policy Committee, please see Section C.3 of the HMIS Policies and Procedures herein.

F. Article 6: Responsibilities of Partner Agencies

Partner Agencies are homeless service providers in Contra Costa County that have agreed to be an active contributor to the CONTRA COSTA HMIS. Partner Agencies must sign a Memorandum of Understanding between H3 and the Partner Agency (Partner Agency HMIS MOU). Partner Agencies are responsible for designating a staff person to oversee the HMIS activities of users within the agency and serve as a liaison with the HMIS Lead (hereinafter referred to as the Partner Agency HMIS Agency Administrator or Agency Administrator). Partner Agencies must develop internal policies and procedures to ensure its staff complies with the HMIS policies, procedures, governance charter, or other related HMIS agreements. Partner Agencies must hold client information in HMIS in strict confidence and adhere to all confidentiality policies related to client data. For a full description of the roles and responsibilities of Partner Agencies, please see Section C.4 of the HMIS Policies and Procedures herein.

III. Part Two: HMIS Policies and Procedures

HMIS Policies and Procedures

A. Purpose

The HMIS Policies and Procedures (Policies and Procedures) provides policies, procedures, and guidelines that govern HMIS operations, as well as responsibilities for Partner Agencies and End Users.

B. Governing Principles

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

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

C. Roles and Responsibilities

1. Contra Costa CoC

H3 as the CoC Lead Agency for the Contra CoC is responsible for:

- **Designations:**
  - Designating the HMIS Lead Agency: The Research, Evaluation, and Data (RED) team at H3 has been designated as the HMIS Lead Agency
  - Designating a single information system as the official HMIS software for the geographic area: Clarity Human Services has been designated as the official HMIS software
- **Governance Charter:**
  - Executing an HMIS governance charter and regularly monitoring compliance with that charter
- **HMIS Policies and Plans:**
  - Reviewing, revising, and approving all HMIS policies, procedures, standards, and governance documents, HMIS privacy plan, security plan, data quality plan, as well as any updates to these policies or plans
  - Along with HMIS Lead Agency, developing and enforcing community level data quality plan and standards
- **HMIS Monitoring:**
  - Ensuring that HMIS is managed and administered in compliance with all applicable regulations, as well as CoC policies, protocols, and goals
  - Ensuring consistent participation in HMIS and promoting participation in non-participating agencies
  - Regularly monitoring agency and program participation and milestones and making reports available to CoC membership (along with HMIS Lead)
  - Authorizing release of aggregate system-wide data on homelessness within the CoC for required reporting or counts (along with the HMIS Lead)
  - Ensuring adherence by agency staff with HMIS data and system security protocols the CoC and HUD HMIS Data and Technical Standards (along with HMIS Lead and Partner Agencies)
- **HMIS Oversight:**
  - Overseeing guardianship of client data by ensuring appropriate policies, procedures, and standards are in place governing access, use and disclosure of records containing protected identifying information
  - Supporting the HMIS Lead in providing regular training to Partner Agencies and End Users. Trainings may include client confidentiality and privacy training, performance measurement training, business practices that support HMIS policies training, and program funding training
  - Supporting the HMIS Lead in ensuring that appropriate agreements are executed and enforced such as Agency Participation agreements, Data Sharing agreements, HMIS End-User agreements, and client consent agreements

2. HMIS Lead Agency

H3's Research, Evaluation, and Data (RED) Team as the HMIS Lead Agency is responsible for:

- **HMIS Operation and Maintenance:**
  - Day-to-day operations and maintenance of HMIS

- Ensuring all software and supporting services are updated, patched and otherwise maintained
- Serving as liaison to Clarity Human Services on behalf of the CoC and Partner Agencies
- Overseeing software license administration, including adding and removing Partner Agency HMIS Administrators or End Users

- **End User Training and Support**:
  - Providing initial and on-going HMIS training, support and technical assistance to all Partner Agencies. 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
  - Regularly reviewing HMIS service requests, activities, deliverables, and resolutions
  - Managing and maintaining mechanisms for soliciting, and analyzing feedback from end users program managers, agency executive directors, and individuals experiencing homelessness
- **Monitoring and Reporting:**
  - Regularly monitoring agency and program participation and milestones and making reports available to CoC membership (along with CoC Lead)
  - With cooperation from the Partner Agencies, completing any required aggregate data reporting and extraction on behalf of the CoC, including Annual Performance Reports (APRs), Annual Homeless Assessment Report (AHAR), Longitudinal Systemwide Analysis Report (LSA), and Annual Point-in-Time Counts (PIT)
- **Compliance and Enforcement of HMIS Policies and Plans and MOU**:
  - Ensuring that all Partner Agencies comply with standards provided in this Policies and Procedures document, including those specifically provided in the Privacy, Security & Data Quality Plans by working with Partner Agency HMIS Administrators to ensure adherence by agency staff
  - Taking appropriate measures as a result of noncompliance by Partner Agency of these HMIS Policies and Procedures or the Memorandum of Understanding between H3 and Partner Agency, such as implementing a progressive corrective action plan or suspending Partner Agency's access to HMIS until issue has been resolved
- **Security**:
  - In addition to any duties and responsibilities included in the HMIS Security Plan, the HMIS Lead Agency shall be responsible for making all reasonable efforts to maintain and secure client records, HMIS, and supporting services.
  - **User Credentials**: The HMIS Lead 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 HMIS Lead 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 HMIS Lead 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 HMIS Lead will be responsible for making all reasonable efforts to ensure the highest level of data quality possible, including developing and enforcing data quality plans and policies.
  - **Universal Data Elements**: The HMIS Lead 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 HMIS Lead 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 HMIS Lead 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 HMIS Lead 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 reflect the first day of service in the program.Exit dates should recflect the last day of residence, or for non-residential programs, the last day a service was provided.
- **Data Quality Reports**:
  - HMIS Lead Agency supports Partner Agency Administrators to regularly run data quality reports that indicate levels of data entry completion, consistency with program model, and timeliness as compared to the community data quality standards.
  - The HMIS Lead Agency provides technical assistance and training in response to data quality reports.
  - The HMIS Lead Agency may disseminate these data quality reports to the Council on Homelessness or HMIS Policy Committee for community planning and improvements

- **HMIS Participation:**
  - The HMIS Lead maintains documentation of the number of participating agencies using HMIS, regularly reviews and monitors HMIS coverage rates of the CoC, and engages with non-participating agencies to address barriers to participating
  - The HMIS Lead Agency provides reports of participating agencies at least annually to the HMIS Policy Committee
  - The HMIS Lead Agency ensures that appropriate agreements are executed and enforced such as Agency Participation agreements, Data Sharing agreements, HMIS End-User agreements, and client consent agreements

RED Team Roles and Responsibilities	
Role	**Responsibilities**
Research and Evaluation Manager	• Oversees HMIS development, processes, and deliverables • Conducts system level and program level data analysis and evaluation activities to determine impacts and inform effective practices • Develops plans for improvement related to data collection, data analysis, and system/program evaluations • Develops outcomes and indicators that will be used to monitor program performance. • Prepares analytic and statistical reports on operations and activities of the homeless continuum of care • Plans, prioritizes, assigns, supervises, and reviews the work of staff responsible for developing and implementing program applications, program deliverables and/or health assessments • Monitors performance and compliance with applicable specifications, rules, regulations and laws related to research projects; and ensures quality and timeliness of work performed • Oversees and supports data collection practices and privacy and confidentiality across the CoC program
Planner/Evaluator II	• Gathers, tabulates and analyzes HMIS data relative to client demographics, service provisions, and system effectiveness • Conducts complex research and evaluation program studies that may have department-wide/system-wide implications • Helps determine the type of evaluation needed or desired and employs the appropriate research design

	• Conducts outcome evaluations to measure client changes and process evaluations and/or management audits of issues involving policies, procedures, work-flow and regulatory compliance • Develops and revises forms and questionnaires for gathering data and chooses statistical method for displaying results • Reviews collected data, interprets findings and makes conclusions and recommendations based thereon • Assess resources available to address and identify problems and barriers to achieving objectives
HMIS System Administrator	• Facilitates strategic planning around the HMIS. Determine rollout strategy and prioritization among agencies within continuum • Establishes policy and procedures around data use and data dissemination and reviews these policies and procedures annually • Reviews and monitors adherence to established policies and ensure security, confidentiality and quality of information within or exported system • Manages the ongoing implementation and usage of the HMIS system on behalf of the Continuum of Care • Coordinates training and ongoing support with each agency, to ensure users are properly trained. Perform data analysis and reporting as required by each agency. • Resolves local technical issues within the continuum and facilitate problem resolution with any agency experiencing difficulties with software or system • Serves as single point of contact between the Continuum of Care and the HMIS vendor • Oversees submission of HMIS federal reports (PIT, HIC, SPM, LSA) • Create user manuals, technical documentation, and data collection and migration tools • Responsible for recordkeeping of Partner Agency HMIS MOUs and data sharing agreements
HMIS Data Analysts	• Generates and build reports and dashboards using HMIS reporting tools. Use statistical methods to analyze HMIS program-level and system wide data to track client and service outcomes • Identify and recommend new ways to streamline program operations and processes using data • Work with partner agencies to outline specific data needs and translate to useful reports • Provide administrative support to the Homeless Program office including drafting user manuals, creating forms, and generating reports as needed • Oversees HMIS user licenses
HMIS Quality Assurance (QA) and Training Coordinator	• Runs and reconciles reports to ensure system data quality and timeliness. Create quality assurance procedures and generate reports as needed • Provides and/or coordinate trainings to support the quality and accessibility of the HMIS system • Provides 1st tier HMIS troubleshooting and technical support to program staff. • Facilitates technical assistance forums with agency administrators on HMIS operations and policy development • Oversees program compliance to HMIS policies and procedures and HUD Data Standards
HMIS Data Clerk	• Enters and updates client data in the HMIS • Runs and reconciles reports to ensure system data quality and timeliness • Documentation in case records and files to ensure the written record of work performed, including completion of information entered into the database.

	• Collaborates with Program Evaluator to analyze data, write reports, and develop infographics

3. HMIS Policy Committee

The HMIS Policy Committee is responsible for:

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

4. Partner Agencies (PA)

Partner Agencies are responsible for:

- **Adherence with all HMIS Policies and Procedure and Related Agreements**
  - Adhering with all policies and procedures documented in the HMIS Policies and Procedures herein
  - Enforcing HMIS Policies and Procedures through agency level policies and procedures.
  - Signing and complying with all terms provided in the Partner Agency HMIS MOU, the Partner Agency User Agreement, Partner Agency HMIS Administrator Agreement, and any applicable HMIS forms and documents
- **Client Data and Confidentiality**
  - Abiding by all federal and state laws and regulations and with all HMIS Policies and Procedures relating to the collection, storage, retrieval, and dissemination of client information
  - Collecting and maintaining records of all required Standardized Client Informed Consent & Release of Information Authorization forms in accordance with the HMIS Policies and Procedures herein
- **Network Operations**
  - Notifying the HMIS Lead Agency HMIS System Administrator promptly of any difficulty with system software, access to database, or related problems; at no time will the Partner Agency contact the software vendor directly
  - Maintaining their agency internet connectivity and computer equipment in such a manner as not to disrupt continuity of project participation
- **Data Entry and Quality**
  - Collecting all mandatory data elements and striving to collect maximum data elements for consenting clients

- Entering or transferring data into the system as provided in the HMIS Data Quality and Monitoring Plan
- Assuring the accuracy of information entered into the system. Any information updates, errors, or inaccuracies that come to the attention of the Partner Agency will be corrected by the Partner Agency. If necessary, the HMIS Lead Agency must be notified of any corrections that cannot be made by the Partner Agency.
- Monitoring data quality through regular data quality reports that indicate levels of data entry completion, consistency with program model, and timeliness as compared to the community data quality standards
- Developing program specific interview guidelines that include the Standardized Intake Form, the Client Informed Consent & Release of Information Authorization form and HMIS Privacy Notice and any additional elements the agency wishes to collect.
- Partner Agency Executive Director accepts responsibility for all records entered by their agency
- Ensuring that Partner Agency personnel do not knowingly enter erroneous information into the HMIS and conducting regular audits to ensure compliance with this requirement
- Not altering or amending information in the database that is entered by another Partner Agency .
- Maintaining copies of signed client Release of Information forms, either electronically in HMIS or, if physical copies, stored in a secure location for the entire duration the document is effective.

- **Security**
  - Limiting HMIS access to authorized users and following all protocols for monitoring those users and prohibiting shared passwords and accounts.
  - Providing the HMIS Lead Agency with the names of all staff members who have access to the HMIS (End Users) and certifying that such End Users are trained to have access to this information according to the provisions of this HMIS Policies and Procedures and the Partner Agency HMIS MOU. The HMIS Lead Agency may deny access to the system for the purpose of investigation of any suspicion of breached confidentiality.
  - Designating one person to act as the Partner Agency HMIS Agency Administrator (Agency Administrator) for the purpose of managing all communications with the HMIS Lead Agency. The Partner Agency will provide the HMIS Lead Agency with the name and title of the staff member designated.
  - Agency Administrator will ensure that all staff issued a User ID and Password to enter the system sign and abide by Partner Agency User Agreement and complete required confidentiality training.
  - Maintaining records of all Partner Agency User Agreements signed by staff, volunteers and other persons issued a User ID and Password.
  - Not transmitting security information and network policies to non-members of the HMIS in any manner.
  - Developing an internal process for the violation of any of the HMIS information security protocols.
  - Maintaining up-to-date virus and firewall protection at each workstation operating HMIS.
- **Training**
  - Ensuring all agency End Users are properly trained and authorized to use the system in accordance with the HMIS Policies and Procedures.
  - Ensuring that Agency Administrator regularly attends the HMIS Lead Agency monthly HMIS Policy Committee meetings, along with periodic update trainings and stay current with the HMIS Policies and Procedures.
  - Assigned Agency Administrator holds responsibility to communicate any updated HMIS information to all staff and volunteer HMIS End Users at his/her Partner Agency.
- **HMIS User License Fees and Module Costs**
  - Covering all applicable fees associated with user licenses being utilized by Partner Agency. User license fees will be invoiced by HMIS Lead Agency based on the current pricing, as provided by Bitfocus. License fees are established by Bitfocus once annually.
  - Covering the cost of additional HMIS modules requested by Partner Agency specific to Agency needs.

Partner Agency Organization Roles and Responsibilities	
Roles	**Responsibilities**
Partner Agency Executive Director	• Act as authorizing agent for the Partner Agency HMIS MOU • Designation of Agency Administrator • Agency compliance with HMIS Policies and Procedures • Agency level HUD reporting
Partner Agency HMIS Agency Administrator (Agency Administrator or AA)	• Authorizing agent for Partner Agency User Agreements • Keeper of Partner Agency User Agreements • Keeper of executed Client Informed Consent forms • End user licenses • Authorizing agent for user ID requests • Ensure staff workstations are compliant with HMIS Policies and Procedures and HUD requirements • End user adherence to workstation security policies • Ensure sufficient internet connectivity and security • Detecting and responding to violations of the HMIS Policies and Procedures • Provide first-level End User support • Maintain Agency/Program Data in HMIS Application • Data quality monitoring, including running regular data quality reports • Quality assurance • Provide ongoing training to End Users
Agency Staff (End User)	• Safeguard client privacy through compliance with confidentiality policies • Data collection, data entry, and development of dashboards and reports as specified by training and other documentation.

D. 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 HMIS Lead 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) for all relevant projects with sufficient data stored in HMIS in compliance with the latest HUD guidance.
- **Annual Longitudinal Systemwide Analysis Reports:** The Agency shall prepare and submit Annual Longitudinal Systemwide Analysis Reports (LSA) 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.
- **System Performance Measures:** The Agency shall prepare and submit the annual System Performance Measures (SPM) to HUD.
- **Housing Inventory Count (HIC) and Point In Time (PIT):** The Agency shall prepare and submit the Housing Inventory Count (HIC) and the Point In Time (PIT) annually or as required by HUD.

E. Operating Policies and Procedures

1. HMIS Participation

Policies

- Agencies participating in the CONTRA COSTA HMIS must abide by the governing principles of the CONTRA COSTA HMIS, the HMIS Policies and Procedures herein, and adhere to the terms and conditions of the Partner Agency HMIS MOU.
- If applicable, Partner Agency shall pay a participation fee charged by the HMIS Lead Agency as specified in Partner Agency HMIS MOU.

Procedures

a) Confirm Participation

1. In order to become a Partner Agency, the agency shall complete the Contra Costa HMIS Application Form, which will be reviewed by the HMIS Lead and CoC Lead. If the application is accepted, Partner Agency will need to execute a Partner Agency HMIS MOU and an Agency Administrator Agreement.
2. The Partner Agency shall confirm their participation in the CONTRA COSTA HMIS by submitting a signed Partner Agency HMIS MOU to the HMIS System Administrator.
3. The HMIS System Administrator will obtain the co-signature of H3 Division Director.
4. The HMIS System Administrator will maintain a file of all signed MOUs.
5. The H3 System Administrator will update the list of all Partner Agencies and make it available to the project community The list of Partner Agencies that participate in HMIS is included in Attachment A of the Client Informed Consent & Release of Authorization, which can be found at https://www.cchealth.org/hmis.

b) Voluntary Termination

1. If a Partner Agency no longer wants to participate in HMIS, the Partner Agency shall inform the HMIS System Administrator in writing of its intention to terminate its agreement to participate in CONTRA COSTA HMIS.
2. The HMIS System Administrator will provide a 30-Day Notice and inform the CoC Lead Agency, the HMIS Policy Committee, and as necessary, Council on Homelessness.
3. The HMIS System Administrator will revoke access of the Partner Agency End Users 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 HMIS System Administrator will keep all termination records on file with the associated Memorandums of Understanding.
5. Any fees paid for participation in the CONTRA COSTA HMIS will not be refunded.
6. The Partner Agency understands and accepts any ramifications of not participating in the CONTRA COSTA HMIS.

c) Lack of Compliance and Involuntary Termination

1. When the HMIS System Administrator determines that a Partner Agency has failed to comply with the HMIS Policies and Procedures herein or is otherwise in violation of the terms of the partnership as specified in the Partner Agency HMIS MOU, the HMIS Lead Agency will notify the Partner Agency Executive Director and the Agency Administrator to resolve the conflict(s).
2. The HMIS Lead Agency may implement a Corrective Action Plan with the Partner Agency which may include additional training, reporting, and ongoing monitoring requirements until

the issues have been resolved. However, if offense is severe enough, the HMIS Lead Agency may terminate the Partner Agency's access immediately.

3. If the Partner Agency does not follow the Corrective Action Plan, the HMIS Lead Agency may terminate Partner Agency's participation in HMIS.
    i. The Partner Agency will be notified in writing of the intention to terminate their participation in the CONTRA COSTA HMIS.
    ii. The HMIS System Administrator will revoke access of the Partner Agency staff to the CONTRA COSTA HMIS.
    iii. The HMIS System Administrator will keep all termination records on file with the associated Memorandums of Understanding.

d) List of Partner Agency Primary Contacts

1. The Partner Agency shall designate a primary contact for communications regarding the CONTRA COSTA HMIS by submitting a Partner Agency HMIS Administrator Agreement to the HMIS System Administrator.
2. The HMIS System Administrator will maintain a file of all signed Partner Agency HMIS Administrator Agreements and verify the designated Agency Administrator annually.
3. The HMIS System Administrator will maintain a list of all assigned Agency Administrators and make it available to the HMIS Lead project staff.
4. The Partner Agency may designate a new or replacement primary contact in the same manner as above.

e) Site Security Assessment

1. Prior to allowing access to the CONTRA COSTA HMIS, the Partner Agency Executive Director (or designee), Agency Administrator, and the HMIS System Administrator will review and assess the security measures and protocols in place to protect client data. This review shall in no way reduce the responsibility of Partner Agency's information security, which is the full and complete responsibility of the agency, its Executive Director, and Agency Administrator.
2. Partner Agencies shall have the latest version of virus protection software on all computers that access HMIS and comply with Section 9 Workstation Security below.

2. End User Authorization & Passwords

Policies

- Agency Staff participating in the CONTRA COSTA HMIS shall abide by the governing principles of the CONTRA COSTA HMIS, the HMIS Policies and Procedures herein, and adhere to the terms and conditions of the Partner Agency User Agreement.
- End User Licenses
    - The Agency Administrator is the only Partner Agency staff member that is authorized to request licenses on behalf of End Users.
    - The Agency Administrator must only request user access to HMIS for those staff members that require access to perform their job duties (End Users).
    - All End 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 Partner Agency User Agreement).
- Passwords
    - 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.
    - Written information pertaining to user access (e.g., username and password) may not be stored or displayed in any publicly accessible location.

- New User IDs must require password change on first use.
- Passwords must consist of at least 8 characters and must contain a combination of lowercase letters, uppercase letters, numbers, and symbols [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 not use or include the username, the HMIS name, or the HMIS vendor's name.
    - Passwords must not consist entirely of any word found in the common dictionary or any of the above spelled backwards.
- Passwords must be changed every 180 days. Once 180 days has passed, End Users will be prompted to change their passwords at their next log-in.
- After four consecutive unsuccessful attempts to login, the account will be locked for three hours. If the End User cannot wait three hours, they may contact the HMIS Lead Agency to gain access sooner.

Procedures

a) Workstation Security Assessment

1. Prior to requesting user access for any staff member, the Agency Administrator will assess the operational security of the user's workspace to ensure compliance with Section 9 Workstation Security below.
2. The Agency Administrator will confirm that workstation has up to date virus and firewall protection properly installed and that a full-system scan has been performed within the last week.

b) Request New User ID

1. When the Agency Administrator identifies a staff member that requires access to CONTRA COSTA HMIS, the Agency Administrator must notify the RED Team by emailing H3REDteam@cchealth.org with the following information: name of staff person, position, start date, and email address. The RED Team will provide new user training to the prospective end user. Training and any associated coursework must be completed prior to receiving an end user license.
2. At the time of the training, the prospective end user must read and sign the Partner Agency User Agreement and return it to the Agency Administrator.
3. The HMIS System Administrator will create the new User ID as specified and notify the User ID owner of the temporary password via email.

c) Change User Access

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

d) Reset Password

1. When a user forgets their password, they may use the "Forgot Password" link provided in the login screen. Instructions are then emailed to the email address on file. Users should ensure that their email address in Clarity is kept up to date.
2. After four consecutive unsuccessful attempts to login, the account will be locked for three hours. If the End User cannot wait three hours, they may contact the HMIS Lead Agency at H3REDteam@cchealth.org to gain access sooner.
3. If a user has reason to believe that someone else has gained access to their password, they must immediately reset their password in Clarity or notify their Agency Administrator.

e) Termination of User Access

1. If an End User no longer requires access to HMIS, for example if the user leaves the agency or otherwise becomes inactive, their HMIS license must be de-activated.
2. The Partner Agency must notify the HMIS System Administrator within three (3) days after an End User is no longer employed at the agency or no longer needs access to HMIS. The Partner Agency shall provide the name of the staff member and the date of departure or date of deactivation of their HMIS license.
3. The HMIS System Administrator will revoke access of the specified End Users to the CONTRA COSTA HMIS.

f) Lack of Compliance and Involuntary Termination

1. Partner Agencies must develop and implement internal policies and procedures to monitor its End User's compliance with the HMIS Policies and Procedures herein or the terms of the Partner Agency User Agreement. The Partner Agency's internal policies should include disciplinary actions for lack of compliance with these documents.
2. The actions of the End Users are ultimately the responsibility of the Partner Agency. If an End User has been found to be noncompliant with any of the policies and procedures, Agency Administrators shall take corrective action steps with the End User. The HMIS Lead Agency may be available for guidance and support as needed.
3. If the End User continues to be out of compliance, the HMIS System Administrator must deactivate the staff User IDs.
4. End Users will be immediately terminated if they have breached confidentiality of information in CONTRA COSTA HMIS.

3. Collection and Entry of Client Data

Policies

- Client Data must be gathered according to the policies, procedures and confidentiality rules meeting the minimum threshold of HUD data standards and the CoC's HMIS data standards.
- Client Data will only be shared with Partner Agencies if the Client provides verbal or written consent (see Procedures below).
- Client Data will be entered into the HMIS in a timely and accurate manner in compliance with the guidelines set in the HMIS Data Quality Plan.
- Hardcopy or electronic files will continue to be maintained according to individual program requirements.
- Data imports require authorization from both the CoC and HMIS Lead as they may impact data integrity and increase the likelihood of duplication of client files in the system.
- Any authorized data imports will be the responsibility of the Partner Agency.
- Partner Agencies are responsible for the accuracy, integrity, and security of all data input by said agency. The HMIS Lead Agency will periodically monitor for Partner Agencies data quality compliance.
- **Note that services may NOT be denied if Client refuses to sign the ROI or declines to state any information.** Partner Agencies 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.
- **Domestic Violence Dedicated Programs**
    - Victim Service Providers (VSPs) whose primary purpose is to serve victims of domestic violence, are prohibited from participating in HMIS by the Violence Against Women Act (VAWA) and HUD. In addition, providers who receive funding (either through a direct grant or subgrant) from the Family Violence Prevention and Services Act, Office for Victims of Crime, Office on Violence Against Women, and Specialized Housing and Services for

Victims of Human Trafficking are prohibited from entering client PII into HMIS. These agencies are required to use a comparable database and are responsible for meeting the requirements of the comparable database.

- **Non-Homelessness Data**
  - The data inputted and stored in HMIS shall align with the purpose of CONTRA COSTA HMIS, which is to serve as a central database to collect, track, analyze and report uniform client and activity data related to the provision of shelter, housing, and services to individuals and families experiencing homelessness and at risk of homelessness within the Contra Costa CoC region. Data that does not align with or serve this purpose shall not be inputted in HMIS.

Procedures

a) Obtaining Informed Consent & Release of Information (ROI)

1. Client consent to share their data within HMIS must constitute INFORMED consent. The burden rests with the intake counselor to inform the Client before asking for consent.
2. Partner Agencies must explain the contents of the Client Informed Consent & Release of Information Authorization (ROI) and the Contra Costa County's Continuum of Care HMIS Privacy Notice (HMIS Privacy Notice) to the Client prior to entering client information into HMIS. During this explanation, Partner Agencies should summarize the following information:
   a. ***What HMIS is*** - an internet-based database that is used by homeless service organizations across the Contra Costa CoC to record and store client-level information
   b. ***Why the Partner Agency Uses it***
      i. Efficiently coordinate the most effective services and resources for Clients
      ii. Better understanding homelessness in the community
      iii. Assess the types of resources needed in the local area
      iv. Track whether needs are being met in the community
   c. Security
      i. Only specific staff who have signed an agreement to maintain the security and privacy of your information and participate in training courses can access HMIS.
      ii. HMIS is protected by passwords and encryption technology.
      iii. HMIS must adhere to HUD Technical and Data Standards and other local, state and federal privacy laws
   d. *How their personal information may be shared and disclosed*
      i. Coordinate services with other providers in the CoC
      ii. Creating aggregated de-identified data to a third party like HUD
      iii. Cooperate with law enforcement for a legitimate law enforcement purpose based on valid warrant or subpoena
      iv. Full list of permissible disclosures is available in the HMIS Privacy Notice
   e. Clients Rights
      i. No client information will be released to another agency without written or verbal consent from the Client. However, aggregate system wide data that does not contain any client specific identifying data may be shared with internal and external agents without specific permission.
      ii. Client has the right to not answer questions, unless admission to the program requires it.
      iii. Client has right to access their record.
      iv. Clients can't be refused services if consent is not provided.
      v. Clients can revoke consent at a later date.
   f. *Benefits for Clients*
      i. Clients will not have to repeat their story to multiple agencies

ii. Case managers can use information in HMIS to link Client to appropriate resources in the community

3. The Client may sign a hard copy or electronic copy (on-screen signature) of the ROI. Once the client signs the ROI, the Partner Agency must document the ROI in the client's HMIS record.
    a. All written consent forms must be stored in a client's case management file for record-keeping and auditing purposes. The Partner Agency may store the hard copy in their internal files, but must provide the address of the hard copy file in the client's HMIS record and store this copy for the entire duration the document is effective; or
    b. Preferably, the Partner Agency can use the electronic ROI form within HMIS, or may scan and upload the hard copy and attach to the client's HMIS record.
4. Partner Agencies must ensure that hard copy ROIs are stored in a location that is locked and not accessible to the general public.
5. The ROI is valid for ten (10) years. When the ROI expires after 10 years and the client's data is still active in HMIS, then Partner Agencies must obtain a new signed ROI from the client. Client information is stored in the HMIS indefinitely unless the client requests their data to be revoked.

b) Obtaining Verbal Consent

1. A signed written ROI is the preferred method of obtaining client informed consent; however, verbal consent is permitted under the following circumstances:
    a. Client's verbal consent is obtained through one-door registration, 211, or another hotline or dispatch call-center.
    b. If verbal consent is obtained, Partner Agencies must make reasonable attempts to collect written consent upon Client's arrival into the program or through subsequent meetings with the client.
2. **Exception:** Phone registration and dispatch programs may enter client information without consent but must lock the record in HMIS. Upon client's arrival into the program, written consent must be obtained in order to unlock their record.

c) Consent for Minor Children

1. Partner Agencies must obtain consent to input a minor's data into HMIS from the minor's parent or legal guardian.
2. The minor's consent must be documented on the head of household's ROI.

d) Client Refuses to Consent

1. Clients cannot be refused services solely based on their refusal to participate in HMIS.
2. If the Client refuses to provide verbal or written consent, the Partner Agency must not share the Client's PII with any other partner agencies. Partner Agencies must lock the Client's HMIS record. The steps on how to lock a Client's record is provided during End User Training. Within 6 months of the Client's initial refusal, Partner Agencies should make one additional attempt to confirm whether the Client wishes to sign an ROI.

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 HMIS Lead 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 HMIS Lead

Agency understands that federal rules restrict use of the information to criminally investigate any alcohol or drug abuse patients.

- 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 or otherwise permitted under the Privacy Notice.
- Client shall be given a printout of all data relating to them upon written request and five (5) 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 five (5) 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 five (5) 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 (see Section 3).
- Each Partner Agency Executive Director is responsible for their agency's internal compliance with the 2004 HUD Data and Technical Standards. Agency Administrators and End Users must safeguard and maintain strict confidence over information in CONTRA COSTA HMIS.

Procedures

a) HMIS Privacy Notice

1. Partner Agencies must post the HMIS Privacy Notice (available in both English and Spanish) at their facility in a place conspicuous and accessible to clients.
2. Prior to asking the Client to review and sign the ROI, Partner Agency staff must review the HMIS Privacy Notice with the Client (see Section 3).
3. Partner Agencies must provide a copy of the HMIS Privacy Notice to the Client upon request.

b) Client Revocation of Consent

1. A Client may revoke consent for data sharing at any time. When Client makes such request, the Partner Agency staff should provide the HMIS Client Revocation Form to the Client. The Partner Agency staff shall complete the bottom of the HMIS Client Revocation Form with the HMIS Client Unique ID and forward the form securely to the RED Team.
2. Partner Agency staff shall inform the Client that only information going forward will not be shared. PII that the Client previously authorized to be shared cannot entirely be removed from the HMIS database and will remain accessible to the limited number of organizations that provided the Client with direct services.

5. Client Complaint

Policies

- Clients will file complaints with Partner Agencies. Partner Agencies must have written complaint procedures that can be provided to client upon request. Any unresolved complaints may be escalated to the CoC Lead Agency according to the CoC Complaint Process. For HMIS matters, the CoC Lead Agency may work with the HMIS Lead Agency to resolve the complaint.
- Partner Agencies complaint procedures must follow the guidelines and requirements under the CoC Complaint Process.

Procedures

a) Partner Agency Complaint Process

1. Clients will submit a complaint directly to Partner Agencies with which they have a complaint in accordance with the Partner Agency's internal complaint policies and procedures.
2. Upon client request, Partner Agencies must provide a copy of their complaint procedure and the HMIS Policies and Procedures along with the Contra Costa Continuum of Care Complaint Form (CoC Complaint Form). Partner Agencies shall explain that the CoC Complaint Form should be used only if the matter cannot be resolved by the Partner Agency's internal complaint procedure or if the Client believes that filing a complaint through the Partner Agency is inappropriate.
3. The Partner Agency will be responsible to answer any questions and complaints regarding the HMIS. A record of all complaints and any attempts made to resolve the issue must be kept in file for two (2) years. If the complaint is resolved, Partner Agencies will include the date and a brief description of the resolution.

b) CoC Complaint Process

1. If the Partner Agency is unable to resolve the problem or if the client believes that filing a complaint directly with the Partner Agency is not appropriate based on the circumstances, the client must complete the CoC Complaint Form outlining the date of incident, name of parties involved, description of the incident, and their contact information for follow-up. If the client needs assistance, Partner Agencies must forward a copy of the completed CoC Complaint Form to the CoC Manager.
2. The CoC Lead Agency will review and determine the need for further action based on the procedures outlined in the CoC Complaint Process.

6. Data Quality

Policies

- Data quality refers to the timeliness, completeness, and accuracy of information collected and reported in CONTRA COSTA HMIS. All data entered into the HMIS database must meet minimum data quality standards. End Users will be responsible for the quality of their data entry and must adhere to the specific requirements in the Contra Costa CoC Data Quality and Monitoring Plan (DQMP).
- **Data Timeliness:** End Users must enter all universal data elements and program-specific data elements within the specified time provided in the DQMP.
- **Data Completeness:** All data entered into the system must be complete, unless otherwise authorized by the HMIS Lead, following data collection standards set by the 2020 HUD HMIS Data Standards.
- **Data Accuracy:** All data entered shall be collected and entered in a common and consistent manner across all programs to ensure that all data entered into HMIS is an accurate 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.

Procedures

1. Partner Agencies must collect and enter as much relevant client data as possible for the purposes of providing services to that client.
2. All End Users 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. All data must be input into HMIS within the specific number of days based on program type as provided in the DQMP.
3. The HMIS System Administrator will conduct quarterly checks for data quality.
4. Any patterns of error or missing data will be reported to the Agency Administrator. Agency Administrators must adhere to the data quality monitoring and reporting requirements laid out in the DQMP.
5. End Users will be required to correct the identified data error and will be monitored for compliance by the Agency Administrator and the HMIS Administrator.

6. End Users may be required to attend additional training on data quality as needed.

7. Aggregate Data Access

Policies

- The Partner 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 Partner Agency shall use only unidentified, aggregate data.
- The HMIS Lead Agency may also provide anonymous aggregate data for reporting purposes, research purposes, and to policy makers, service providers, advocates, and consumer representatives. The underlying goal of sharing aggregate data is to address and end homelessness.

Procedures

- The Partner Agency is responsible for ensuring that reporting access is maintained at the proscribed levels for agency clients, non-agency clients, and aggregate information reporting.
- Any requests for aggregate data must be directed to the HMIS Lead Agency using the following form on the H3 website: https://cchealth.org/h3/coc/reports.php#Requests.

8. 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.
- **Research and Electronic Data Exchange:** Agencies exporting data from HMIS must certify that the same privacy and security rights promised to their clients are met on the destination system. If the destination system operates under less restrictive rules, the client must be fully informed and approve this transfer. The Partner Agency must have the ability to restrict transfers to only those clients that approve the exchange.

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.
- Partner Agencies shall have internal policies prohibiting transmission of material in violation of any federal or state regulations, this includes but is not limited to: copyrighted material, material legally judged to be threatening or obscene, and material considered protected by trade secret.
- Partner Agencies shall have internal policies that prohibit profanity, offensive language, malicious information or discriminatory comments based on race, ethnicity, religion, national origin, disability, age, gender, or sexual orientation into the database.

9. Workstation Security

Policies

- The Agency Administrator is responsible for preventing degradation of the whole system resulting from viruses, intrusion, or other factors under the agency's control.
- The Agency 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).
- The Agency Administrator is responsible for communicating all procedures to End Users regarding proper workstation configuration and protection against unauthorized access to HMIS by others.
- Additional security policies are included in the HMIS Data Security Plan.

Procedures

a) Computer Security

1. At a minimum, any workstation accessing the HMIS System shall have anti-virus software with current virus definitions (24 hours) and frequent full-system automated scans (weekly).
2. Partner Agency shall ensure that its computers and networks are equipped with secure firewalls, which are updated regularly automatically. Firewalls must be placed between any computer and internet connection for the entire network.
3. All workstations and computer hardware along with agency network equipment must be stored in a secure location, such as a locked office where only authorized users have access. If computers are in a public area, they must be staffed at all times. When not in use, computers must be secure and not usable by unauthorized users. Computers should automatically turn on a password protected screen saver when the workstation is temporarily not being used.

b) Hard Copy Security

1. Partner Agency staff must supervise at all times any paper or other hard copy generated by or for the HMIS that contains PII when the hard copy is in a public area.
2. When Partner Agency staff is not present, the paper files must be secured and locked in areas that are not publicly 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.
4. Documents printed from HMIS must be sent to a printer in a secure location where only authorized users have access.

10. Training

Policies

- Partner Agencies must ensure its End Users are properly trained and authorized to use the system in accordance with the HMIS Policies and Procedures herein.
- The Agency Administrators must regularly attend the HMIS Lead Agency monthly HMIS Policy Committee meetings, along with periodic update trainings and stay current with the HMIS Policies and Procedures.
- The Agency Administrator holds responsibility to communicate any updated HMIS information to all staff and volunteer HMIS End Users at his/her Partner Agency.
- End Users may also be required to participate in periodic trainings to maintain their end user license.

Procedures

a) Training

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

- Data Privacy, Security, & Confidentiality
- HUD HMIS Data Standards
- End User Training

- Specific Modules

b) Agency Administrator Training

The HMIS Lead Agency will provide training to Agency Administrators who are then responsible for relaying that training to End Users within his or her agency. Training will be done virtually or in a group setting, where possible to achieve the most efficient use of time and sharing of information between agencies. Training will include:

- End User training
- Running package reports
- Creating customized reports

c) Ongoing Training

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

- Agency Administrator Training
- End User Training
- Data Privacy, Security, & Confidentiality
- Data Quality Monitoring and Reporting
- HUD HMIS Data Standards
- Specific Modules

11. Technical Support

Policies

- Support requests include problem reporting, requests for enhancements (features), or other general technical support.
- End Users shall submit support requests to their Agency Administrator (email is suggested).
- End Users shall not submit requests to software vendor.
- End Users shall not submit requests directly to the HMIS Lead Agency without specific invitation. All requests to H3 shall be submitted to the Agency Administrator, who may then escalate to the HMIS Lead Agency, who may then escalate to vendors as appropriate.
- The HMIS Lead will only provide support for issues specific to the CONTRA COSTA HMIS software and systems.

Procedures

a) Submission of Support Request

1. End User encounters a problem or originates idea for improvement to system or software.
2. End User creates a support request to Agency Administrator.
3. The Agency Administrator, upon receipt of a support request, shall make reasonable attempts to resolve the issue directly with End User.
4. If the Agency Administrator is unable to resolve the issue and determines that the problem is specific to CONTRA COSTA HMIS software and systems, the Agency Administrator may contact the HMIS Systems Administrator or the AA may submit a technical support request, including program set up or program modification using the following link: https://airtable.com/shr07VkUci0rE8Rqt.
5. The HMIS 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 HMIS 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, the HMIS System Administrator will provide instructions via email to Agency Administrator.

12. Changes to this and other Documents

Policies

- The CoC and HMIS Lead along with 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 an annual basis.

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. The HMIS System Administrator will maintain a list of proposed changes.
4. The list of proposed changes will be discussed by the HMIS Policy Committee, subject to line item excision and modification. This discussion may occur at an in-person or virtual meeting.
5. The HMIS Policy Committee will recommend annual proposed changes to the CoC's governing body, Council on Homelessness, for approval prior to implementation.
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 the HMIS System Administrator. The Agency Administrator (cc to E.D.) shall also ensure circulation of the revised document within their agency and compliance with the revised Policies and Procedures by all End Users.

IV. Appendix A: HMIS Data Security Plan

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 Agency 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 HMIS Governance Charter and HMIS 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 Partner Agency 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. Written information pertaining to user access (e.g., username and password) may not be stored or displayed in any publicly accessible location.
e. New User IDs must require password change on first use.
f. Passwords must consist of at least 8 characters and must contain a combination of letters and numbers(required by software). (Refer to the HUD Data and Technical Standards Final Notice (July 2004) for additional guidance.)
g. Passwords must not use or include the username, the HMIS name, or the HMIS vendor's name.
h. Passwords must not consist entirely of any word found in the common dictionary or any of the above spelled backwards.

i. Passwords must be changed every 180 days. Once 180 days has passed, End Users will be prompted to change their passwords at their next log-in.
j. After four consecutive unsuccessful attempts to login, the account will be locked for three hours. If the End User cannot wait three hours, they may contact the HMIS Lead Agency to gain access sooner.

Agencies participating in the CONTRA COSTA HMIS shall commit to abide by the governing principles of the CONTRA COSTA HMIS and shall adhere to the terms and conditions of this partnership as detailed in the Partner Agency Memorandum of Understanding and the HMIS Governance Charter and HMIS Policies and Procedures.

Prior to allowing access to the HMIS, the Agency Administrator will agree to review and assess the security measures in place to protect client data. The HMIS System Administrator will meet Partner Agency Executive Director (or designee), Program Manager/Administrator and Agency 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 Agency Administrator.

Termination of User Access

If an End User no longer requires access to HMIS, for example if the user leaves the agency or otherwise becomes inactive, their HMIS license must be de-activated. The Partner Agency must notify the HMIS System Administrator within three (3) days after an End User is no longer employed at the agency or no longer needs access to HMIS. The Partner Agency shall provide the name of the staff member and the date of departure or date of deactivation of their HMIS license. The HMIS System Administrator will revoke access of the specified End Users to the CONTRA COSTA HMIS.

Lack of Compliance and Involuntary Termination

Partner Agencies must develop and implement internal policies and procedures to monitor its End User's compliance with the HMIS Policies and Procedures herein or the terms of the Partner Agency User Agreement. The Partner Agency's internal policies should include disciplinary actions for lack of compliance with these documents.

The actions of the End Users are ultimately the responsibility of the Partner Agency. If an End User has been found to be noncompliant with any of the policies and procedures, Agency Administrators shall take corrective action steps with the End User. The HMIS Lead Agency may be available for guidance and support as needed. If the End User continues to be out of compliance, the HMIS System Administrator must deactivate the staff User IDs. End Users will be immediately terminated if they have breached confidentiality of information in CONTRA COSTA HMIS.

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 HMIS Governance Charter and HMIS

Policies and 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 with current virus definitions (24 hours) and frequent full-system automated scans (weekly). 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 and secure firewall 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 Partner 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 Partner Agency Administrator maintains hardware, software and PPI in a secure environment, protected by a Firewall. Firewalls must be updated regularly automatically and must be placed between any computer and internet connection for the entire network. 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

All workstations and computer hardware along with agency network equipment must be stored in a secure location, such as a locked office where only authorized users have access. If computers are in a public area, they must be staffed at all times. When not in use, computers must be secure and not usable by unauthorized users. Computers should automatically turn on a password protected screen saver when the workstation is temporarily not being used.

Disaster Protection and Recovery

HMIS is contained on mariaDB databases which are run on a 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 databases are automatically backed up nightly and stored on another secure server.

Bitfocus, the vendor of Clarity Human 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 the Agency 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. Partner 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 Partner Agency staff is not present, the paper files must be secured in areas that are not publicly 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.
4. Documents printed from HMIS must be sent to a printer in a secure location where only authorized users have access.

Data Breach Procedure

In the event a Partner Agency becomes aware of a potential system security or client confidentiality breach, the Agency HMIS Administrator shall notify the HMIS Lead immediately by sending an email to H3REDteam@cchealth.org. The HMIS Lead will begin an investigation to determine the probability that PPI has been compromised. If the data breach was caused by human error, such as unintentionally including a non-covered HMIS entity in an email, or physical theft of a device containing PPI, the information must be redacted/wiped immediately to the extent possible. Partner agency staff should not directly contact the client(s) affected by the breach unless directed to do so by the HMIS Lead.

V. Appendix C: HMIS Client Data & Privacy Plan

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.

Obtaining Informed Consent & Release of Information (ROI)

Client consent to share their data within HMIS must constitute INFORMED consent. The burden rests with the intake counselor to inform the Client before asking for consent. Partner Agencies must post the HMIS Privacy Notice (available in both English and Spanish) at their facility in a place conspicuous and accessible to clients and must provide a copy of the HMIS Privacy Notice to clients upon request.

Partner Agencies must explain the contents of the Client Informed Consent & Release of Information Authorization (ROI) and the Contra Costa County's Continuum of Care HMIS Privacy Notice (HMIS Privacy Notice) to the Client prior to entering client information into HMIS. During this explanation, Partner Agencies should summarize the following information:

1. ***What HMIS is*** - an internet-based database that is used by homeless service organizations across the Contra Costa CoC to record and store client-level information
2. ***Why the Partner Agency Uses it***
    a. Efficiently coordinate the most effective services and resources for Clients
    b. Better understanding homelessness in the community
    c. Assess the types of resources needed in the local area
    d. Track whether needs are being met in the community
3. ***Security***
    a. Only specific staff who have signed an agreement to maintain the security and privacy of your information and participate in training courses can access HMIS.
    b. HMIS is protected by passwords and encryption technology.

c. HMIS must adhere to HUD Technical and Data Standards and other local, state and federal privacy laws

4. ***How their PPI may be shared and disclosed***
    a. Coordinate services with other providers in the CoC
    b. Creating aggregated de-identified data to a third party like HUD
    c. Cooperate with law enforcement for a legitimate law enforcement purpose based on valid warrant or subpoena
    d. Full list of permissible disclosures is available in the HMIS Privacy Notice
5. ***Clients Rights***
    a. No client information will be released to another agency without written or verbal consent from the Client. However, aggregate system wide data that does not contain any client specific identifying data may be shared with internal and external agents without specific permission.
    b. Client has the right to not answer questions, unless admission to the program requires it.
    c. Client has right to access their record.
    d. Clients can't be refused services if consent is not provided.
    e. Clients can revoke consent at a later date.
6. ***Benefits for Clients***
    a. Clients will not have to repeat their story to multiple agencies
    b. Case managers can use information in HMIS to link Client to appropriate resources in the community

The Client may sign a hard copy or electronic copy (on-screen signature) of the ROI. Once the client signs the ROI, the Partner Agency must document the ROI in the client's HMIS record. All written consent forms must be stored in a client's case management file for record-keeping and auditing purposes. The Partner Agency may store the hard copy in their internal files, but must provide the address of the hard copy file in the client's HMIS record; or the Partner Agency may scan and upload the hard copy or upload the electronic signed copy to the client's HMIS record. Partner Agencies must ensure that hard copy ROIs are stored in a location that is locked and not accessible to the general public.

The ROI is valid for ten (10) years. When the ROI expires after 10 years and the client's data is still active in HMIS, then Partner Agencies must obtain a new signed ROI from the client.

Obtaining Verbal Consent

A signed written ROI is the preferred method of obtaining client informed consent; however, verbal consent is permitted under the following circumstances:

1. Client's verbal consent is obtained through one-door registration, 211, or another hotline or dispatch call-center.

2. If verbal consent is obtained, Partner Agencies must make reasonable attempts to collect written consent upon Client's arrival into the program or through subsequent meetings with the client.

Exception: Phone registration and dispatch programs may enter client information without consent but must lock the record in HMIS. Upon client's arrival into the program, written consent must be obtained in order to unlock their record.

Consent for Minor Children

Partner Agencies must obtain consent to input a minor's data into HMIS from the minor's parent or legal guardian. The minor's consent must be documented on the head of household's ROI.

Client Refuses to Consent

Clients cannot be refused services solely based on their refusal to participate in HMIS. If the Client refuses to provide verbal or written consent, the Partner Agency must not share the Client's PII with any other partner agencies. Partner Agencies must lock the Client's HMIS record. Within 6 months of the Client's initial refusal, Partner Agencies should make one additional attempt to confirm whether the Client wishes to sign an ROI.

Adherence to Other Privacy Laws

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 Partner Agency will use or disclose personal information for activities described in this part of the notice. The Partner 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 a client.
b. For payment or reimbursement of services for the participating organization.
c. For administrative purposes, including but not limited to HMIS system administrator(s) and developer(s), and for legal, audit, personnel, and oversight and management functions.
d. For creating de-identified PPI to disclose to a third party.
e. To cooperate with a law enforcement official for a legitimate law enforcement purpose, consistent with applicable law and standards of ethical conduct, provided that such disclosure should be only the minimum amount of information necessary for the law enforcement official's immediate purpose, and the law enforcement official provides a

lawful justification for the request (such as a warrant).

f. As authorized by law, for victims of abuse, neglect, or domestic violence.
g. To prevent a serious threat to health or safety.
h. For academic research purposes but never published in an identifiable form.
i. Other uses and disclosures of your PPI can be made with your written consent.
j. A coroner, medical examiner or funeral director for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law.
k. Where disclosure is required by law.
l. To cooperate with legitimate requests for data from California State agencies that will be used for research, policy development, and/or creation of state-wide data warehouses.
m. For other purposes consistent with the ultimate goal of improving housing and homeless services that do not unduly burden the privacy rights of clients.

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 Partner Agency must allow individuals to inspect and have a copy of their personal information that is maintained in HMIS in accordance with the HMIS Privacy Notice. Each agency must offer to explain any information that is not understood. Clients can exercise this right by making a written request to their social worker/case manager. Social workers/case managers can obtain assistance from their Agency Administrator, who can connect with the RED Team for additional support.

Within five (5) business days of the written request, the Partner Agency must provide the individual with:

- A correction of inaccurate or incomplete PPI;
- A copy of the consent form;
- A copy of the full HMIS Privacy Notice;
- A copy of the individual's HMIS records; and,
- A current list of participating organizations that have access to your HMIS data.

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

Revocation

Clients may revoke their consent for sharing information in HMIS at anytime. Agencies shall facilitate this revocation by providing the client with the Client Revocation Form. Agencies should assist clients with completing the form if needed. Once the client has completed the form, Agencies should email the form securely to H3REDteam@cchealth.org.

Upon receipt of the revocation request, the HMIS Lead shall remove the Client's PPI from the HMIS database and prevent further PPI from being added. Partner Agency staff shall inform the Client that only information going forward will not be shared. PPI that the client previously authorized to be shared may not entirely be removed from the HMIS database and may remain accessible to the limited number of organizations that provided the Client with direct services.

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

Victim Service Providers are prohibited from entering data into HMIS. Other agencies must take extra precautions when handling data from victims of domestic violence, dating violence, sexual assault, and stalking. A Partner Agency may disclose PPI about an individual whom 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 Partner Agency that makes a permitted disclosure about a domestic violence incident must promptly inform the individual that a disclosure has been or will be made, except if 1) the Partner Agency, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or 2) the Partner Agency would be informing a personal representative (such as a family member or friend), and the Partner 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 Partner Agency in the exercise of professional judgment.

VI. Appendix D: HMIS Privacy Notice

Contra Costa County's Continuum of Care:
Homeless Management Information System (HMIS) PRIVACY NOTICE

THIS PRIVACY NOTICE EXPLAINS UNDER WHAT CIRCUMSTANCES WE MAY SHARE AND DISCLOSE YOUR INFORMATION FROM CONTRA COSTA COUNTY'S HMIS. THIS NOTICE ALSO EXPLAINS YOUR RIGHTS REGARDING YOUR CONFIDENTIAL INFORMATION.

Brief Summary

[Effective 8/18/2020]
[Version 2]

This notice describes the privacy policy of the [Name of Homeless Agency]. We may amend this policy at any time and amendments may affect information obtained by the covered homeless organization before the date of change. We collect personal information only when appropriate. We may use or disclose your information to provide you with services. We may also use or disclose it to comply with legal and other obligations. We assume that you agree to allow us to collect information and to use or disclose it as described in this notice, based on your consent provided in the CLIENT INFORMED CONSENT & RELEASE OF INFORMATION AUTHORIZATION. You can inspect personal information about you that we maintain. You can also ask us to correct inaccurate or incomplete information. You can ask us about our privacy policy or practices. We respond to questions and complaints. Read the full notice for more details. Anyone can have a copy of the full notice upon request.

Contra Costa County's Continuum of Care:
Homeless Management Information System PRIVACY NOTICE

Full Notice

[Effective 8/18/2020]

[Version 2]

Please review this notice carefully. If you have difficulty reading this notice, please ask for assistance.

A. What This Notice Covers

1. This notice describes the policy and practices of [Name of Homeless Agency]. Our main office is at [address, email/web address, telephone].
2. The policy and practices in this notice cover the process of protected personal information for clients of [Name of Homeless Agency].

Our organization collects and shares information about individuals who access our services. The information is confidentially stored in a local electronic database called the Contra Costa County Homeless Management Information System (CCC HMIS). The CCC HMIS securely records information (data) about persons accessing housing and homeless services in Contra Costa County. This Privacy Notice explains how we process confidential personal information that we collect about you and your family. This confidential information is referred to as Protected Personal Information (PPI). We are required to protect the privacy of your PPI by complying with the privacy practices described in this Privacy Notice.

B. Why We Collect and Share Information

When you request or receive services from this program, we ask for information about you.
This information helps us continuously improve services to people experiencing homelessness by:

1. Efficiently coordinating the most effective services for you and your family;
2. Better understanding homelessness in your community;
3. Assessing the types of resources needed in your local area; and
4. Tracking whether needs are being met in your community.

By collecting your information for HMIS, we are able to generate aggregate statistical reports requested by the Department of Housing and Urban Development (HUD).

C. The Type of Information We Collect and Share in the HMIS

We collect and share PPI and general information obtained during your intake assessment, contact assessments while engaged with services, and exit assessments, including but not limited to:

1. Name and contact information
2. Social security number
3. Birthdate
4. Demographic information such as gender and race/ethnicity
5. History of homelessness and housing (including current housing status and where and when services have been accessed for both you and your family members)
6. Self-reported medical history including any mental health and substance use issues
7. Case notes and services
8. Case manager's contact information
9. Income sources and amounts; healthcare benefits; and non-cash benefits
10. Veteran status
11. Disability status
12. Household composition
13. Emergency contact information
14. Domestic violence history
15. Criminal history

D. How Your PPI Is Secured in the HMIS

The information you provide is entered into a computer program called the Homeless Management Information System (HMIS). This computer program operates over the Internet and is managed by the HMIS lead agency in Contra Costa County: the Health, Housing and Homeless Services Division of Contra Costa Health Services (H3). This agency is required by law to maintain the privacy of protected personal information and to provide you with notice of their legal duties and privacy practices with respect to protected personal information. The HMIS uses many security protections to ensure the safety and confidentiality of your information.

Your information is protected by passwords and encryption technology. Each HMIS user and participating organization must sign an agreement to maintain the security and privacy of your information and participate in training courses to ensure protection and security of your information. If an HMIS user or participating organization violates the agreement, their access rights may be terminated and may be subject to further penalties pursuant to applicable state and federal privacy laws.

E. How PPI May Be Shared and Disclosed

Unless restricted by other laws, the information we collect can be shared and disclosed under the following circumstances:

1. To provide or coordinate services to a client.
2. For payment or reimbursement of services for the participating organization.
3. For administrative purposes, including but not limited to HMIS system administrator(s) and developer(s), and for legal, audit, personnel, and oversight and management functions.
4. For creating de-identified PPI to disclose to a third party.
5. To cooperate with a law enforcement official for a legitimate law enforcement purpose, consistent with applicable law and standards of ethical conduct, provided that such disclosure should be only the minimum amount of information necessary for the law enforcement official's immediate purpose, and the law enforcement official provides a lawful justification for the request (such as a warrant).
6. As authorized by law, for victims of abuse, neglect, or domestic violence.
7. To prevent a serious threat to health or safety.
8. For academic research purposes but never published in an identifiable form.
9. Other uses and disclosures of your PPI can be made with your written consent.
10. A coroner, medical examiner or funeral director for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law.
11. Where disclosure is required by law.
12. To cooperate with legitimate requests for data from California State agencies that will be used for research, policy development, and/or creation of state-wide data warehouses.
13. For other purposes consistent with the ultimate goal of improving housing and homeless services that do not unduly burden the privacy rights of clients.

F. Providing Your Consent for Sharing PPI in the HMIS

In addition to providing you this Privacy Notice, we will also obtain your written consent through a Release of Information unless an exception applies. *Exception*: In a situation where we are gathering PPI from you during a phone screening, street outreach, or community access center sign-in, your verbal consent can be used to share your information in HMIS. If we obtain your verbal consent, you will be requested to provide written consent during your initial assessment. If you do not appear for your initial assessment, your information will remain in HMIS until you revoke your consent in writing.

You have the right ***not*** to provide protected personal information to an agency. You may exercise your right of privacy by not answering any or all of the personal questions asked by the agency. You will not be denied services for not answering questions regarding your protected personal information, unless federal statute requires that your data must be shared as a condition of program participation.

G. How to Revoke Your Consent for Sharing Information in the HMIS

You may revoke your consent at any time. Your revocation must be provided either in writing or by completing the *Client Revocation of Consent form*. You may receive help to complete this form. Upon receipt of your revocation, we will remove your PPI from the shared HMIS database and prevent further PPI from being added. The PPI that you previously authorized to be shared cannot be entirely removed from the HMIS database and will remain accessible to the limited number of organization(s) that provided you with direct services.

Your Rights to Your Information in the HMIS

You have the right to receive the following, no later than five (5) business days of your written request:

1. A correction of inaccurate or incomplete PPI;
2. A copy of your consent form;
3. A copy of the full CCC HMIS Privacy Notice;
4. A copy of your HMIS records; and
5. A current list of participating organizations that have access to your HMIS data.

We are required to explain any information that you may not understand (HMIS Privacy and Security Standards §4.2.5). You can exercise these rights by making a written request, either written by yourself or by someone designated on your behalf. You can either email or mail your written request:

- Email written request to: H3REDteam@cchealth.org;

or

- Mail the request to: H3 Research, Evaluation, and Data Team
  2400 Bisso Lane, Suite D, 2nd Floor
  Concord, CA 94520

Your Privacy Rights Regarding Your Information in the HMIS

If you believe your privacy rights have been violated, you may send a written grievance, either written by yourself or someone you designated on your behalf, to [Enter agency name, email address, and/or mailing address]. This agency has the responsibility to notify the HMIS lead agency (H3) of the grievance within 3 business days of receipt. You will not be retaliated against for filing a grievance. If your grievance is not resolved to your satisfaction, you may send a written grievance appeal to the Research, Evaluation, and Data team at H3REDteam@cchealth.org. If there is a need to escalate the complaint/grievance, it will be taken to the Contra Costa Oversight Committee for further investigation. The Oversight Committee will review the complaint/grievance and provide recommendations on the solution. If a solution can be reached, the grievance is closed.

Amendments to this Privacy Notice

The policies in this notice may be amended by the HMIS lead agency at any time. These amendments may affect information obtained by this organization before the date of the change. Amendments regarding use or disclosure of PPI will apply to information (data) previously entered in HMIS, unless otherwise stated. All amendments to this privacy notice must be consistent with the requirements of the federal HMIS privacy standards. This organization must keep permanent documentation of all privacy notice amendments.

VII. Appendix E: Supporting Forms and Documents

Supporting Forms and Documents

The following forms and documents related to HMIS operations can be found at: https://www.cchealth.org/hmis.

- Contra Costa Data Quality Monitoring Plan
- Client Informed Consent and Release of Information Authorization
- Release of Information Client Benefits
- Standardized Intake Form, Update, and Exit Forms
- Contra Costa County's Continuum of Care HMIS Privacy Notice
- HMIS Client Revocation of Consent
- Contra Costa HMIS Data Collection Guide
- Clarity HMIS Workflow End User Training (Clarity's User's Manual)