

NORCAL CONTINUUM OF CARE CA-516

HMIS Policies – Final November 2025

TABLE OF CONTENTS

Introduction	2
HMIS Use and Purpose	2
HMIS Software and Administration	3
HMIS Policies and Procedures	3
HMIS Governing Principles	3
Key Support Roles and Responsibilities	4
HMIS Lead Agency	4
HMIS Administration Responsibilities	5
HMIS/Coordinated Entry System Committee	5
Agencies Participating in Coordinated Entry	6
HMIS Partnership Violations and Termination	8
Data Transfer/Downloads for Terminated Agencies	10
HMIS Data Quality and monitoring	10
HMIS Administrator Technical Support	11
HMIS User Training	11
Hardware, Connectivity, and Security:	12
Workstation Access Restrictions	13
Workforce Access Restrictions	13
Establishing End-user Access	13
Data Access and Password Policies	14
Rescind User Access	14
HMIS Privacy Plan	15
HMIS Definitions	15

INTRODUCTION

The NorCal Homeless Management Information System (HMIS) serves the NorCal Continuum of Care (CA-516). Congress has established a national goal that all communities should be collecting an array of data about homelessness, including unduplicated counts of individuals who are homeless, their use of services and the effectiveness of local assistance systems. HMIS is a valuable resource because of its capacity to integrate and deduplicate data from all participating homeless assistance and homeless prevention programs in a Continuum of Care. Aggregate HMIS data can be used to understand the size, characteristics and needs of the homeless population at the local, state and national levels. The HMIS Data and Technical Standards are issued by the U.S. Department of Housing and Urban Development (HUD).

The NorCal HMIS is operated by Pathways/MISI. The roles and responsibilities described in this document will primarily be fulfilled by the Continuum of Care, the HMIS Lead Agency, and HMIS Partner Agencies (referred to as Contributing Homeless Organizations or CHOs).

Every active HMIS End User is to comply with the **HMIS Data and Technical Standards: Final Notice** (published by the U.S. Department of Housing and Urban Development in 2004). Failure to comply with the HUD standards carries the same consequences as failure to comply with these Policies and Procedures. In any instance where these Policies and Procedures and Security Plan are not consistent with the HUD HMIS Standards, the HUD Data Standards take precedence. Should inconsistencies be identified, please immediately notify the HMIS Lead Agency.

The Norcal HMIS Policies will be reviewed annually or as required by HUD Data Standard Updates.

HMIS USE AND PURPOSE

The purpose of the NorCal HMIS is to serve as an integrated network of homeless and other services providers that use a central database to collect, track and report uniform information on client needs and services. HMIS not only meets federal and state requirements but also enhances service planning and delivery. The long-term vision of HMIS is to enhance Partner Agencies' collaboration, service delivery and data collection capabilities. Accurate information will put the collaborative in a better position to request funding from various sources and help better plan for future needs.

The fundamental goal of the NorCal CoC HMIS is to document the demographics of homelessness in the seven-county NorCal Continuum of Care according to the HUD HMIS Data Standards. It is then the goal of the summarized HMIS data to assist the U.S. Congress in providing an annual estimate of homelessness, including demographic characteristics, service use patterns, and the national capacity to house homeless persons. HMIS data also assists local Continuums of Care and participating agencies to improve identify regional service gaps, track services trends and outcomes and inform resource allocation.

Data is gathered via intake interviews and program participation will be used to generate summarized reporting. This data may also be analyzed to provide unduplicated counts and de-identified information to policy makers, service providers, advocates, and consumer representatives.

The HMIS serves as a community-level homeless information system and is supported by the following Federal and State partners:

- Department of Housing and urban Development – (HUD) for Continuum of Care (CoC), Emergency Solutions Grants (ESG), Housing Opportunities for Persons with AIDS (HOPWA)
- Department of Health and Human Services (HHS): PATH, RHY

- Department of Veteran's Affairs (VA): SSVF GPD programs

State of California HMIS mandated use includes the following funding streams:

- Emergency Solutions Grant (ESG)
- Housing Support Program (HSP)
- Bringing Families Home (BFH)
- Housing and Disability Advocacy Program (HDAP)
- Behavioral Health Bridge Housing (BHBH)

HMIS SOFTWARE AND ADMINISTRATION

The NorCal Continuum of Care has chosen WellSkye Community Services (ServicePoint) as its HMIS Vendor. ServicePoint is a cloud-based HMIS to be the platform or record. HMIS access is limited to agencies who have executed CoC HMIS participation agreements and end-users who have been authorized by the HMIS Administrator to have met required privacy and security, data collection, entry and reporting requirements.

The NorCal CoC has designated Pathways/MISI located in Atlanta, GA to serve as the HMIS Administrator effective September 18, 2025. Administration of the HMIS will be evaluated annually in August. The HMIS Administrator will be tasked with preparing regular and ad-hoc reports, analysis, presentations and other documents as assigned by the CoC Executive Board.

The Administrator will also fulfill the following roles:

- Develop and implement security procedures and protocols related to data collection, entry and use by the NorCal CoC.
- Manage local HMIS to the HUD Data Standards including updates.
- Provide System Administration in accordance with the HUD System Administrator Checklist.
- Develop and deliver HMIS end-user training programs encompassing data collection requirements, data management and quality best practices, and helpdesk support.

HMIS POLICIES AND PROCEDURES

For Agency Projects where HIPAA applies, HIPAA requirements take precedence over both the HUD HMIS Data Requirements (as specified in those requirements) and these Policies. Agencies and their related programs are responsible for ensuring HIPAA compliance. Governing Principles establish the values that are the basis for all policy statements and subsequent decisions.

Operating Procedures include the HMIS Privacy Plan and Security Plan which provides policies and steps necessary to control the operational environment and enforce compliance in project participation, workstation security, user authorization and passwords, training of collection and entry of client data, release and disclosure of client data, training, compliance, and technical support.

The HMIS Data Quality Plan provides specific rules on data management that need to be maintained in the system per funding source including timeframes for when data needs to be entered and updated.

HMIS GOVERNING PRINCIPLES

All End Users are expected to read, understand, and adhere to the HMIS Policies. Described below are the overall governing principles upon which all decisions pertaining to the NorCal HMIS are based. Clients can control what is being entered into HMIS. Each individual client can grant informed consent, limited data sharing, be entered anonymously or revoke consent to their information at any time.

End Users are expected to securely and accurately enter in client's data into HMIS, understanding the data is valuable and sensitive in nature. Policies written in this document will ensure protection of this asset from accidental or intentional unauthorized modification, destruction or disclosure. End Users shall strive for the highest

possible degree of data quality, as poor data quality can lead to reduction in funding for service and may affect the other NorCal counties resource opportunities.

Information Confidentiality:

The rights and privileges of clients are crucial to establishing trust in the HMIS initiative. These policies will ensure clients' privacy without impacting the delivery of services. 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 as such.

Data Integrity:

Clients must have confidence that their personal information is securely protected and used only to enhance service delivery. Effective community planning depends on accurate and timely HMIS data, supported by sound policy and informed decision-making. Funders also monitor data quality closely and may reduce or withhold funding if data accuracy or completeness is poor. Additionally, HMIS data is governed by legal and ethical standards at every level, requiring that all users maintain the highest level of data integrity and confidentiality.

KEY SUPPORT ROLES AND RESPONSIBILITIES

CoC Executive Board

NorCal's primary decision-making group regarding homelessness services, housing and funding is the NorCal Executive Board. This fifteen-member public- private decision-making body will align funding and policy to address homelessness throughout the County and serves as the county's Continuum of Care Board to address HUD requirements.

The Board must be a subset of the CoC membership that is established in accordance with the CoC regulations governing board composition (Please refer to the NorCal Continuum of Care Governance Charter for details).

Responsibilities of the CoC Executive Board:

- a. Designate a single HMIS for the NorCal CoC geographic area and designate an eligible applicant to manage
- b. Promote and/or enforce HMIS Participation
- c. Develop and implement strategic plan for HMIS participation and develop data driven solutions
- d. Receives and approves HMIS system-wide information and reports
- e. Monitor performance and evaluate outcomes of the following programs: Emergency Solutions Grant (ESG), Continuum of Care (CoC), Homeless Emergency Aid Program (HEAP), State Homeless Housing Assistance and Prevention (HHAP) Program, and California Emergency Solutions and Housing (CESH)
- f. Review and approve all HMIS plans, forms, standards and governance documents
- g. Establish appropriate performance target by populations and programs
- h. Ensure compliance with federal regulations
- i. Assists Department of Health Services and Provider Agencies to identify and apply for other public and private funding sources for HMIS operations

HMIS LEAD AGENCY

The Lead Agency is responsible for providing support and accountability for the HMIS. TEACH Inc. located in Alturas, Modoc County, serves as the HMIS Lead Agency. The NorCal CoC Executive Board may revisit the HMIS Lead Agency designation at its discretion.

HMIS Lead Responsibilities:

- a. Serve as the Lead Agency for the NorCal Continuum of Care.
- b. Develop, review, and revise all HMIS plans, forms, standards and governance documents.

- c. Oversee and ensure the HUD System Performance Measures, AHAR/Longitudinal System Analysis, and State of California HDIS data submissions meet deadlines and the data contains minimal errors.
- d. Staff the HMIS Committee
- e. Ensure that data is reported accurately and with integrity so that the CoC Executive Board and general public have confidence in the credibility of all reported data
- f. Serves as Liaison and Executes contract with HMIS software vendor
- g. Oversee HMIS licensing - procuring, issuing, removal
- h. Oversee contracting and HMIS Administration compliance with the selected HMIS Vendor and Administrator

HMIS ADMINISTRATION RESPONSIBILITIES

Project Management:

Oversees the general operations of the HMIS project and may also supervise HMIS staff. Interacts with CoC leadership, program leadership, and the HMIS Lead agency's leadership. Monitors the ongoing operation of the CoC's HMIS database. HMIS Administration complies with the HMIS System Administrator Checklist to the extent possible.

End-User Support:

- Oversees Help-Desk functions and technical support services
- Monitors and evaluates the quality, timeliness and accuracy of data input and reporting management
- Develops and maintains HMIS documents and sessions in alignment with the current HUD HMIS Data Standards to assist End Users with data collection, entry and basic reporting
- Oversees all training of Provider Agency Leads and End-users
- Supervises internal and external security protocols
- Addresses HMIS platform technical operational issues with the HMIS Vendor
- Reports HMIS Vendor performance issues to the HMIS Committee and/or CoC Executive Board

Data Integrity and Compliance:

The HMIS Administrator holds primary responsibility for ensuring data integrity across the HMIS. This includes establishing and maintaining policies, procedures, and system configurations that promote accurate, complete, and consistent data.

Data Analysis and Reporting:

Analyzes data for the CoC, including non-HMIS data. The HMIS Administrator interprets, visualizes, and presents data to the CoC.

Ensures CoC mandated reporting requirements are met.

- Oversee system-wide reporting.
- Writes detail report specifications based on requests from the User Group and Project Team.
- Generates reports using ServicePoint Report Writer or as warranted the third-party report designer SAP Business Objects.
- Assists Agency End Users to generate program-level agency reporting or raw data sets as requested.
- Serve as the primary contact for communications regarding HMIS users at the agency. Forward information to all agency End Users as appropriate.
- Maintains documentation of custom reports including purpose and scope, business requirements, business logic, data sources, report structures, query parameters and report filters.
- Maintains documentation of Extract, Transform and Load (ETL) processes necessitated by data cleaning efforts or ongoing database management.

HMIS/COORDINATED ENTRY SYSTEM COMMITTEE

The HMIS/Coordinated Entry System (CES) Committee is made up of various members from the NorCal CoC community. The NorCal CoC Executive Board will appoint at a minimum (1) committee member from each county

and one (1) alternate. Committee members are required to attend not less than 75% of scheduled meetings per year. The purpose of these meetings is to establish and enforce HMIS Policies and Procedures; Coordinated Entry Policies and Procedures assist in the planning of all point-in-time counts; review all participating agencies' compliance reports, review all requests for changes to the policies; and plan/participate in compliance monitoring. The HMIS Committee is actively involved in furthering CoC goals.

Committee Description:

To ensure every Participating Agency is compliant with HUD and County mandated Policies and Procedures, it is necessary for each county in the Continuum of Care to be involved in the formulation of these Policies and Procedures. These meetings will give Participating Agencies the opportunity to voice their concerns as well as determine what and how the policies are written and enforced.

Committee Framework:

- The CoC Coordinator in collaboration with the HMIS Committee Chair or Vice Chair will agendize, host, moderate and determine the Committee schedule
- The HMIS Lead will post agendas at least 72 hours prior to the meeting and conduct meetings in accordance with the California Brown Act
- Committee members or interested parties wishing to add items to the Committee Agenda can do so by emailing requests at least one-week prior to the meeting date to: teachinc.modoc@gmail.com
- Changes, additions or deletions to the approved HMIS Policy and Procedures require HMIS/CES Committee approval. All requests must be submitted on a Request for HMIS/CES Policy Change Form to be discussed and considered by the Committee
- The HMIS Lead Agency will distribute minutes of each meeting at least 72 hours before the next scheduled HMIS/CES Committee Meeting

CoC Collaboration:

- HMIS Participating Agencies are strongly encouraged to suggest meeting topics they feel should be discussed
- HMIS Participating Agencies and end-users are encouraged to share ideas and best practices they feel would be of benefit to other End Users

AGENCIES PARTICIPATING IN COORDINATED ENTRY

Participating Agencies should collect data on individuals or families experiencing homelessness that make contact with the Participating Agency. Enrolling those individuals in Coordinated Entry allows HMIS Participating Agencies the ability to count the persons that attempt to enroll in programs/services, even though they may not actually end up receiving those services. The Participating Agency will be able to create reports about the characteristics of these individuals and use this information for a number of reasons. The Participating Agency could use this data to determine if they are being improperly referred or to quantify the additional need for funding.

Partner Agency HMIS Lead

The Partner Agency Technical Administrator is an employee of the HMIS Partner Agency (Agency Executive Director or Executive Director's designee) and is the first point of contact for all service providers for matters relating to HMIS.

Agency Responsibilities:

- Oversee partner agency compliance with the Participation Agreement, End-User Agreements, and all applicable intake forms, data standards and governance documents
- Detect and respond to violations of application HMIS forms, standards and governance documents
- Serve as primary contact for communications regarding the HMIS users at the agency, forwarding information to all Agency End Users as appropriate

- Ensure and monitor internally accurate data collection and reporting by Agency End Users as specified by the HMIS Data Standards or other funder data collection/reporting requirements
- Monitor end-user compliance in regard to client security and privacy
 - a. Responsible for ensuring appropriate user of the HMIS database by Agency designated staff
 - b. Maintain internal data integrity for participating HMIS projects
 - c. Allow HMIS access to qualified end-users based on job description and need for access
 - d. Reviews HMIS Policies and Procedures with all new end-users and reviews with all users at least annually
- Develops and maintains internal policies and procedures to ensure:
 - a. New and continued staff training
 - b. Timely and accurate input of HMIS data
 - c. Personnel procedures addressing violations of the HMIS Code of Ethics.
 - d. Protocols for data access and reporting
- Maintaining agency and program descriptor data in HMIS in accordance with grant agreements and funder HMIS specifications
- Overseeing partner agency compliance with the Participation Agreement, End-User Agreements, and all applicable intake forms, data standards and governance documents
- Internal reporting protocols
- Report unauthorized personnel within three business days of job departure including changes in work role that no longer need HMIS access within three business days to the HMIS Administrator so the unauthorized user may be immediately deactivated

Agency Security Officer:

The Partner Agency Security Officer is an employee of the HMIS Partner Agency. This could be the same employee as Partner Agency Technical Administrator, who monitors security for the workstations.

- Conduct a thorough quarterly review of internal compliance with all applicable HMIS plans, standards and governance documents.
- Completing the Compliance Certification Checklist and forwarding the Checklist to HMIS Coordinator at least annually.
- Continually monitor and maintain security of all staff workstations used for HMIS access.
- Safeguard client privacy by ensuring End User and agency compliance with confidentiality and security policies.
- Investigate potential breaches of HMIS system security and/or client confidentiality and notify the NorCal HMIS Administrator of substantiated incidents.
- Developing and implementing procedures for managing new, retired, and compromised local system account credentials.
- Developing and implementing procedures that will prevent unauthorized users from connecting to private agency networks.
- Ensure proper agency workstation configuration and for protecting their access by all agency users to the wider system.
- Assumes responsibility for integrity and protection of client information entered into the HMIS database.
- Update virus protection software on agency computers that accesses the HMIS database on a scheduled, regular basis.
- Ensure the Agency provides and maintains adequate internet connectivity.
- Monitors End-user compliance in regard to security.
- Is responsible for insuring appropriate use of the database by Provider Agency's designated staff.

Agency End User:

Each agency shall have one or more End Users responsible for timely and accurate entry into the NorCal HMIS. Only authorized parties may be provided access for the following reasons:

- Data entry into the HMIS
- Viewing/editing Client recordings include profile, entry/exit, assessment and services information
- Downloading data applicable to operational projects for that Agency
- Report design
- Agency HMIS administration

End User Responsibilities:

All HMIS users and participating agencies share responsibility for maintaining data integrity. This includes entering data consistently according to established data standards, regularly reviewing and correcting errors, and safeguarding against unauthorized alterations or deletions. Reliable data allows for valid performance measurement, equitable resource distribution, and compliance with federal, state, and local reporting requirements.

- Meet the HMIS Data Quality standards such as data entry timeliness, response accuracy according to the current HUD Data Standards, State of California applicable data quality standards or other funder data quality requirements
- Adhere to HMIS Provider Agency Policies and Procedures
- Prevent unauthorized disclosure of client data
- Report security violations to Agency Administrator
- Maintain end-user login credentials only for that end-users' use, no sharing or login information

HMIS PARTNERSHIP VIOLATIONS AND TERMINATION

After a confirmed report of a HMIS procedural violation, the HMIS Administrator implements action within 24 hours.

- In emergency situations i.e. security breach and/or imminent danger to the database, the HMIS Coordinator immediately contacts and reports to the CoC Coordinator, who has final authority for the impending action
- In all other cases, the HMIS Coordinator implements a course of action outlined in the following steps:

Step 1: Consultation with the Provider Agency

- a. Contacts and discusses the inappropriate practice with the Provider Agency Administrator
- b. Itemizes specific requirements for improvement.
- c. Identifies a time frame for implementation and completion of the corrective measure(s).
- d. Coordinates further training if deemed necessary.
- e. Documents conversation and reports this information to technical support staff for database entry.
- f. Alerts technical support staff to begin monitoring procedures, which remain in place until resolution.

Step 2: Written Warning

- a. If any corrective measures do not happen, or if inappropriate practices continue over multiple months, then the HMIS Coordinator, under the guidance of the Data Committee, and SCDHS Administrators, implements a written warning procedure.
- b. The HMIS Coordinator or an appropriate HMIS staff member (under the HMIS Coordinator instruction) sends a written notice, via certified mail, to the Provider Agency Administrator which includes:
 - An explanation of violations and itemizes specific requirements for improvement as defined through a Corrective Action Plan.
 - A time frame for implementation and completion of the corrective measure(s).
 - A copy of the written summary documenting the HMIS Coordinators, User Group and CoC Coordinator's review of the Provider Agency's profile.

- A training or technical assistance plan, if deemed necessary.
 - Further HMIS actions if the inappropriate practice(s) continue.
- c. The technical support staff archives a copy of the written warning in the Agency's file; the agency receives the original written notice.

Step 3: Sanctions

- a. If the Provider Agency fails to provide satisfactory responses to the written warning within the allotted time period, as defined in the Corrective Action Plan, then the HMIS Coordinator presents the updated Provider Agency file to the Data Committee and NorCal CoC Coordinator.
- b. The HMIS/CES Committee and CoC Coordinator review all previous correspondences and/or Provider Agency corrective action responses and determine sanctions based on the evidence.
- c. The HMIS Coordinator notifies via certified mail the Provider Agency of impending sanctions, the effective date, a copy of the original written notice, a copy of the HMIS Grievance Policy and this policy.
- d. The technical support staff archives a copy of the sanctions notification in the Agency's file; the Agency receives the written notice.

Step 4: Probation

- a. If the Provider Agency fails to provide satisfactory responses to the sanctions within the allotted time period, then the HMIS Coordinator presents the updated Provider Agency file to the Data Committee and SCDHS Ending Homelessness Manager.
- b. The HMIS/CES Committee and CoC Coordinator review all previous correspondence and Provider Agency corrective action responses and determine warranted probation.
- c. The HMIS Coordinator notifies via certified mail the Provider Agency of impending probation and the effective date.
- d. Assigns Technical Support staff to work with and monitor resolution of identified areas of violation.

Notification:

- a. Explains the violation(s) and itemizes specific requirements for improvement.
- b. Identifies assigned HMIS staff, who will work collectively with the Agency Administrator and Executive Director, to determine the reason(s) for ineffective corrective measures and create a timeline for effective resolution.
- c. Includes a copy of the HMIS/CES Committee and CoC Coordinator's review of the Provider Agency's issues.
- d. Explains the change in provider status to Probationary Provider Agency.
- e. The probationary period remains effective until all corrective measures meet the Data Committee and CoC Coordinator's approval and will not persist past one hundred and eighty (180) days from the notification date.
- f. The technical support staff archives a copy of the probation notification in the Provider Agency's file; the Provider Agency receives the original written notice.

Step 5: Suspension

- a. If the Probationary Provider Agency's inappropriate practice(s) continues or reoccurs, and there is no resolution with the HMIS Coordinator and HMIS staff satisfactory to the Data Committee and NorCal CoC Coordinator to being the suspension process.

The HMIS Lead:

- a. Notifies via certified mail the Provider Agency of impending suspension and the effective date.
- b. Assigns appropriate HMIS staff to facilitate data identification and data transfer to another database.
- c. Immediately inactivates all Provider Agency End-user database access.
- d. Reactivates End-user access after receiving written permission via email or fax from the Data Committee and/or the CoC Coordinator.

- e. The HMIS Administration staff archives copies of the Suspension Notice in the Agency's file. The Agency receives the written notice

Step 6: Termination

a. If the Probationary Provider Agency refuses to attend the mandatory meeting or comply with HMIS Policy and Procedures, then SCDHS Ending Homelessness Manager issues an order to the HMIS Coordinator to permanently terminate the Provider Agency access to the HMIS database. HMIS Lead notifies via certified mail the Provider Agency the effective date of termination

DATA TRANSFER/DOWNLOADS FOR TERMINATED AGENCIES

In regard to the Terminated Agency's HMIS data the agency assumes responsibility for the following:

- Submitting a request for their data within 60 days of termination.
- Cost of data transfer to another database
- Paying the HMIS Lead Agency prior to data delivery
- Receipt of the data according to HMIS Vendor's download protocols

Reinstatement Process:

The Terminated Provider Agency may request reinstatement once previous violations have been addressed and corrected.

Terminated Provider Agency:

1. Contacts HMIS Lead Agency for reinstatement.
2. Fills out Reinstatement Corrective Action Plan, which identifies violation(s) and concerns.
3. Provides documented evidence of corrective procedures.
4. Establishes a timeline for completed corrective procedures.

HMIS Administrator:

1. Acknowledges within 24 hours receipt of the Reinstatement Corrective Action Plan via email.
2. Reviews and determines feasibility of Reinstatement Corrective Action Plan.
3. Contacts Provider Agency, within five working days, with any modifications to or approval of the submitted Reinstatement Corrective Action Plan.
4. Assesses corrective process and time-line adherence.
5. Reviews Reinstatement Corrective Action Plan with the Ending Homelessness Manager.
6. Accepts or denies reinstatement. Contacts the Provider Agency when Reinstatement Corrective Action Plan meets satisfactory completion or if further action is required.

CoC Coordinator:

1. Instructs HMIS Administrator to re-activate the Agency Administrator/Executive Director User License when applicable.

HMIS Administrator:

Provides reinstatement date to the Provider Agency. Re-activates Provider Agency's Probationary Status. coordinating time-line dates and corrective changes into the monitoring procedure.

1. Monitors the Reinstatement Corrective Action Plan.
2. Reports outcomes weekly to the HMIS Coordinator.
3. Contacts HMIS Coordinator immediately of any further breaches of Policies and Procedures.
4. Files completed report in Provider Agency file.

HMIS DATA QUALITY AND MONITORING

HMIS Administration will oversee the following elements of NorCal HMIS Data Quality:

- HMIS Administration staff review reviews monthly reports for completeness, accuracy, and consistency to support federal, state and agency-level project performance expectations

- Data quality reports will be reviewed quarterly by the CoC Executive Board or HMIS Committee to ensure performance measures can be met and for transparency
- Document clear processes for correcting data and assist provider agencies to clarify project-level data quality issues
- Oversee data reliability and validity issues before publishing to the CoC Executive Board and Committees, as well as the general public
- Monitor and resolve duplicate client profiles and overlapping project enrollments
- Maintain a Data Quality Management Plan including common errors and correction steps

HMIS End-users will oversee and be responsible for:

- Ensure basic demographic data is captured correctly (entering the full legal name, correct date of birth, and social security number if applicable).
- Use the Client Search function prior to creating any new record; this includes searching the HMIS by name and their social security number if applicable)
- Review existing project enrollments to ensure adherence to Street Outreach policies and that clients are not participating in bed projects simultaneously

HMIS Agency Administrator will:

- Monitor and merge duplicate client records when possible (the Provider Agency can only merge duplicates when both project enrollments are created within their HMIS projects). If the System Administrator cannot merge the duplicate client, the System Administrator will notify HMIS staff by email, including the applicable Client ID's that require merging.

HMIS ADMINISTRATOR TECHNICAL SUPPORT

End-users submit support requests via email to their Partner Agency HMIS Administrator when encountering issues with the HMIS. If the Partner Agency HMIS Administrator cannot resolve the issue with the End-user, the HMIS Administrator will forward the request to the HMIS Lead Agency for resolution.

If the HMIS Administrator is unable to resolve the request, they will escalate the request to the HMIS software vendor as appropriate. Support requests include reporting problems, requests for feature enhancements, or other general technical support. Under no circumstances should End-users submit support requests directly to the HMIS software vendor. The HMIS Lead Agency will only provide support for issues specific to HMIS software and systems.

Agency users may contact NorCal HMIS Administration Support by emailing: support@pathwaysmisi.org

HMIS USER TRAINING

The HMIS Administrator develops and delivers end user training programs to ensure consistent, accurate, and ethical use of the HMIS. Training includes system navigation, data entry standards, privacy and security protocols, and updates to HUD or CoC data requirements. The Administrator also provides ongoing technical assistance and refresher sessions to maintain data quality and user compliance. Standard HMIS training covers the following:

HMIS Client Security and Ethics:

HMIS New User Orientation:

HMIS Reporting Basics including report generation, data extraction, and interpretation to support accurate reporting and performance monitoring.

HMIS Learning Management System: Self-Paced

HMIS End User Recertification:

Continued access without recertification poses a **data security and compliance risk** and can result in HUD findings during monitoring. Annually, or when there is an update, the HMIS Administrator will review current HMIS Data Standards, privacy and security requirements, and local workflow changes.

HMIS Data Collection Assessments:

All HMIS users are required to complete periodic assessments to demonstrate proficiency in system use, data quality, and privacy compliance. These assessments may include quizzes, data entry exercises, or review of mock client records to ensure users understand current HUD data standards and CoC procedures. Successful completion of required assessments is necessary to maintain active HMIS user licenses and system access.

Assessments include all data collection requirements required by HUD, but not be limited to the following:

- Client Profile
- Client Profile Additional Information
- Project Entry
- Project Exit
- Coordinated Entry Assessment
- VI-SPDAT for Individual and Families
- Custom Assessments – examples and available upon request

HMIS Data Queries & Reporting

Generates raw data and reports upon request to support CoC planning, performance monitoring, and compliance. Ensures data accuracy, protects client confidentiality, and follows all HUD and CoC data governance standards.

HMIS Customizations

Agencies may submit requests for custom assessments or reporting through the HMIS Administrator. All requests must clearly describe the purpose, target population, and data elements required to ensure alignment with CoC priorities and HUD data standards.

Custom assessments will be reviewed to confirm they do not duplicate existing tools, conflict with HUD or CoC data collection requirements, or compromise data integrity. Development of new assessments or specialized reporting may require approval from the HMIS/CoC Committee and must be prioritized based on available system resources.

Requests are addressed in the order received, with consideration of project impact and urgency. Agencies may be asked to participate in testing and validation prior to deployment to ensure data quality and usability.

HARDWARE, CONNECTIVITY, AND SECURITY

Malicious codes, delivered through various means, are designed to delete, scramble End-user files/ programs and/or disable specific computer functions. At times a malicious code slows down a computer--- a mere inconvenience; other times, a malicious code causes an entire system to shut down. Since the computer industry progresses rapidly, each Provider Agency must keep current on protective procedures by consulting with computer system experts periodically for the latest in malicious code preventative measures.

Each HMIS Partner Agency must have at least one HMIS Security Officer at all times. This HMIS Security Officer is responsible for preventing degradation of the HMIS resulting in viruses, intrusions, or other factors within the agency's control and the inadvertent release of confidential client-specific information through physical, electronic, or visual access to the workstation. The HMIS Security Officer must meet all the Privacy and Security requirements detailed in the HUD HMIS Data and Technical Standards.

WORKSTATION ACCESS RESTRICTIONS

Agency Workstation Minimum requirements:

- Computer workstations must be connected to the internet to access HMIS.
- Recommended Internet connection: Wired, or Secure Wireless connection
- Recommended Browsers: is compatible with Chrome, Firefox, Edge, and iOS Safari. And must
- have an antivirus with the latest virus
- Access to the HMIS database should only be from pre-determined work terminals. HMIS should
- only be accessed through secure workstations and prohibited on public workstations (libraries, cafes, etc.).

End-user Requirements:

- a. Log-off the HMIS database and close the Internet browser before leaving a work terminal.
- b. Log-off the HMIS database and close the Internet browser prior to surfing the Internet.
- c. Never leave an open HMIS database screen unattended.
- d. Passwords must not be saved on the computer or posted near the workstation. Immediately notify the designated Agency Administrator or the HMIS Coordinator of any suspected security breach.
- e. Printer location – Documents printed from HMIS must be sent to a printer in a secure location where only authorized persons have access.
- f. PC Access (visual) — Non-authorized persons should not be able to see an HMIS workstation screen. Monitors should be turned away from the public or other unauthorized Partner Agency staff members or volunteers and utilize visibility filters to protect client privacy.

WORKFORCE ACCESS RESTRICTIONS

Each participating agency must conduct a criminal background check on each of its Partner Agency HMIS Administrators and Security officers at its own expense. The Partner Agency's Executive Director will evaluate the results of the criminal background checks for any concerns.

To protect the security and integrity of the HMIS system and safeguard the personal information contained therein, the Partner Agency's Executive Director must consider the results of the background check on a case-by-case basis. An individual whose background raises concerns about whether s/he may sufficiently be relied upon to help the HMIS Lead Agency achieve this goal may not initially be given administrative-level access to HMIS.

An individual whose background raises concerns about whether s/he may sufficiently be relied upon to help the HMIS Lead Agency achieve this goal may be enrolled as an HMIS End-user. After at least one year, if the individual demonstrates through proper and safe use of HMIS that the individual is reliable and trustworthy, they may apply to become a Technical Administrator. The results of the background check must be retained in the subject's personnel file by the Technical Administrator. A background check may be conducted only once for each person unless otherwise required.

ESTABLISHING END-USER ACCESS

Licenses are provided to Agency End-Users upon completion of the following:

- a. Completes HMIS New User Orientation, which includes the Security and Ethics Training.
- b. Read, understand and sign the current HMIS Policies and Procedures.
- c. Read, understand, and sign the HMIS End User Code of Ethics Reads and agrees to abide by the HMIS Agency Partnership Agreement.
- d. User agrees to comply with HMIS confidentiality practices.

The HMIS Lead Agency will keep all documents of the completed Agreement.

- a. The End-user will be issued a unique User ID and password, which may not be transferred to one another. Instead, the Partner Agency will request an additional HMIS license, and if one is available, be issued a new User ID.
- b. The User ID's access level is granted based on the end-user's job description

- c. When an Agency Administrator determines a change needs to be made to the User's access, they will notify the HMIS Administrator

DATA ACCESS AND PASSWORD POLICIES

- a. The Agency Administrator contacts the HMIS Coordinator to set up a new End-user and provides a temporary password.
- b. The Agency Administrator communicates this password to the new End-user.
- c. The End-user must change the password after initially logging correctly into the database. Never transmit End-user identification and computer-generated passwords together in one email, fax, telephone call, or other means of communication.
- d. Passwords and usernames must be transmitted separately (e.g., one portion via email and the other via voice) unless physically handed to the End-user, who must destroy the paper transmission upon successfully entering the HMIS database.
- e. The End-user creates a unique password between 8 and 16 characters with a minimum of two numbers. The End-user DOES NOT use a password used for other purposes; this password must be unique.
- f. Passwords shall not include the end-user name, the HMIS name, or the HMIS Vendor's name.
- f. Passwords should not consist entirely of any word found in the common dictionary or any of the above spelled backwards.
- h. Password is space and case sensitive.
- I. Passwords should be changed every 90 days and end-users must create a new password that is different from the original (expiring) password.
- j. Unique Passwords - User IDs are individual, and passwords are confidential. No individual should ever use or allow the use of a User ID that is not assigned to that individual, and user-specified passwords should never be shared or communicated in any format.

Protection of Downloaded HMIS Data:

NorCal HMIS Administrator or the NorCal HMIS Lead assumes no responsibility for the management, protection, and transmission of client-identifying information stored on local agency computers, agency files, and reports. Partner Agency is responsible for any data file or report downloaded from HMIS.

RESCIND USER ACCESS

Partner Agencies will notify the HMIS Coordinator within 24 hours when any user leaves their position or determined no longer needs HMIS access.

HMIS End User access must be rescinded ASAP when:

When any HMIS user breaches the User Agreement, violates the Governance Policies & Procedures, breaches confidentiality or security, leaves the agency, or otherwise becomes inactive, the Partner Agency HMIS Administrator will deactivate staff User Ids.

The Continuum of Care Executive Board is empowered to permanently revoke End-user access to HMIS for a breach of security or confidentiality.

Special Considerations

Termination or Extended Leave from Employment:

- a. Upon Termination, the Agency Administrator will:
 - Delete the End-user immediately assume all responsibility for deleting their End-users from the HMIS system
- b. Upon extended Leave from employment, the Agency Administrator will:
 - Lock an End-user within five business days of the beginning of an extended leave period greater than 45 days
 - Unlock the End-user upon returning

HMIS PRIVACY PLAN

All HMIS users and participating agencies must comply with federal, state, and local privacy regulations, including HUD's HMIS Data and Technical Standards. Client information may only be collected, used, and shared for purposes directly related to housing and service delivery. Users must obtain and document informed client consent where required, protect all identifying information from unauthorized disclosure, and follow CoC policies for data sharing and release. Any breach of privacy obligations may result in disciplinary action or loss of system access.

HMIS DEFINITIONS

Client: A living individual about whom a Participating Agency collects or maintains protected personal information: (1) because the individual is receiving, has received, may receive, or has inquired about services; or (2) in order to identify service needs, or to plan or develop appropriate services within the CoC.

Continuum of Care (CoC): The group organized to carry out the responsibilities and requirements under 24 CFR part 578 that is composed of representatives of organizations including: nonprofit homeless providers, victim service providers, faith-based organizations, governments, businesses, advocates, public housing agencies, school districts, social service providers, mental health agencies, hospitals, universities, affordable housing developers, law enforcement, organizations that serve homeless and formerly homeless veterans, and homeless and formerly homeless persons to the extent these groups are represented within the geographic area and are available to participate.

CoC Coordinator: The CoC Coordinator oversees the coordination and implementation of the Continuum of Care's housing and service system. This role ensures compliance with HUD requirements, facilitates collaboration among participating agencies, supports CoC governance and planning activities, and oversees performance monitoring and reporting. The CoC Coordinator works closely with the HMIS Lead and other partners to align data, funding, and program strategies that advance the community's goals to prevent and end homelessness.

CoC Program: The Continuum of Care (CoC) Program is a HUD-funded initiative that promotes communitywide planning and coordination to prevent and end homelessness. It supports housing and service projects, fosters data-driven decision-making through HMIS participation, and ensures accountability to federal standards and local performance goals.

Contributory Non-CoC Programs: A program that is neither a homeless assistance program nor a homelessness prevention program that contributes Protected Identifying Information or other client-level data to an HMIS.

HMIS System Administrator: An organization designated by a CoC to operate the CoC's HMIS on its behalf.

Homeless Management Information System (HMIS): The information system designated by NorCal CoC CA 516 to comply with the requirements of HUD used to record, analyze, and transmit client and activity data in regard to the provision of shelter, housing, and services to individuals and families who are experiencing homelessness or at risk of homelessness.

HUD: The federal agency responsible for national housing policy, community development, and homeless assistance programs. It administers funding, establishes regulations and standards, and provides oversight to ensure safe, affordable housing and effective local implementation of programs like the Continuum of Care (CoC) and HMIS.

Administrative Entity: The organization designated to manage the administrative and financial responsibilities of the Continuum of Care. This includes receiving and disbursing HUD CoC Program funds, ensuring compliance with federal regulations, managing subrecipient agreements, and overseeing reporting and auditing requirements. The Administrative Entity also manages the State of

California homeless funding grants.

Participating Agency: An organization that operates a project that contributes data to an HMIS.

Participating Agency HMIS Lead: An individual designated by the Participating Agency Executive Director, or other empowered officer, to act as the Participating Agency HMIS Lead. The Participating Agency HMIS Lead is the liaison between the HMIS System Administrator and the Participating Agency's End Users.

Participating Agency End User: An employee, volunteer, affiliate, associate, and any other individual acting on behalf of a Participating Agency, who uses or enters data into HMIS.

Participating CoC Program: A contributory CoC Program that makes reasonable efforts to record all the universal data elements and all other required data elements as determined by HUD funding requirements on all clients served.

Protected Identifying Information (PII): Information about a Client that can be used to distinguish or trace a Client's identity, either alone or when combined with other personal or identifying information, using methods reasonably likely to be used, which is linkable to the Client.

Security Officer: An individual designated at each Participating Agency to be responsible for ensuring compliance with applicable security standards.

System Administrator: An individual designated by the HMIS System Administrator to act as the System Administrator. The System Administrator is the liaison between the Participating Agencies and the HMIS System Administrator .

Victim Services Provider: A nonprofit or nongovernmental organization including rape crisis centers, battered women's shelters, domestic violence transitional housing programs, and other programs whose primary mission is to provide services to victims/survivors of domestic violence, dating violence, sexual assault, or stalking.

APPENDIX A

NorCal CA 516 Continuum of Care HMIS Request for Policy Addition, Deletion, Change

Agency: _____

Name: _____

Role: _____

Date: _____

I request that the following change(s) be made to the HMIS Policies & Procedures Manual: Change the following existing policy:

Delete or edit the following policy (page number and section title or language):

Add/edit to state the following:

Provide in clear and concise language the policy to be considered by the HMIS Committee to be inserted / deleted in or from the current Policies and Procedures manual. Please be clear and specific.

Policy Revision:

Provide a rationale for the policy change (attach explanation if more space needed):

Procedures or recommended changes to workflows:

Forward recommended changes to the following:

HMIS Lead TEACH Inc. teachinc.modoc@gmail.com and

Pathways/MISI support@pathwaysmisi.org

at least ten (10) business days prior to the HMIS/CES Committee for preparation and consideration