MENDOCINO COUNTY HOMELESS SERVICES CONTINUUM OF CARE HMIS POLICIES AND PROCEDURES

MCHSCOC HMIS Policies and Procedures Manual

APPROVED 01.10.2022

TABLE OF CONTENTS

OVERVIEW

Pursuant to 24 Code of Federal Regulations (CFR) Parts 91, 576, 580, and 583 Interim Rule, this document shall serve as the Homeless Management Information System (HMIS) Policies and Procedures Manual for the Mendocino County Homeless Services Continuum of Care (MCHSCoC), (CA-509).

As a counterpart to MCHSCoC's Governance Charter, this document shall be reviewed, revised, and ratified annually with the governance charter upon a majority vote of all voting members present during the scheduled meeting.

INTRODUCTION

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

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

WHAT IS HMIS

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

WHO USES HMIS

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

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

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

An important exception to the aforementioned entities is victim service providers. Pursuant to 24 CFR Part 578.572, providers assisting victims of domestic violence, dating violence, human trafficking, sexual assault, and stalking victims are prohibited from using HMIS. Rather such providers must use a comparable database. At the time of this writing, the Victim Service Provider Project Sanctuary is expanding their current data collection software to meet the HUD requirements to be an HMIS Comparable Database.

WHY HMIS IS IMPORTANT

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

SECTION 1: HMIS GOVERNANCE STRUCTURE

Mendocino County Homeless Services Continuum of Care (MCHSCoC) HMIS governance structure features a tripartite composition of the following roles:

1. Mendocino County Health and Human Services Agency (HHSA) as Mendocino County Homeless Services Continuum of Care's (MCHSCoC) Lead Agency
2. Mendocino County HHSA as MCHSCoC's HMIS Lead Agency/Grantee
3. Mendocino County Homeless Services Continuum of Care Governing Board HMIS and Performance Measurement Committee (HMIS/PMC)

Pursuant to MCHSCoC's Governance Charter, Mendocino County Health and Human Services Agency (HHSA) serves as the region's Lead Agency, HMIS System Administrator, and as HMIS Lead/Grantee. In addition, and pursuant to this document (Mendocino County Homeless Services Continuum of Care HMIS Policies and Procedures), Mendocino County Health and Human Services Agency (HHSA) serves as the Daily Operator.

MENDOCINO COUNTY CONTINUUM OF CARE (COC) LEAD AGENCY

Pursuant to MCHSCoC's Governance Charter, Mendocino County Homeless Services Continuum of Care Governing Board works with the MCHSCoC committees to appoint the MCHSCoC Collaborative Applicant, MCHSCoC HMIS Lead, and MCHSCoC Coordinated Entry System Lead, which will fulfill the following three major duties:

1. Operate the MCHSCoC
2. With the assistance of the HMIS Performance Management Committee, design and operate a Homeless Management Information System (HMIS)(24 CFR §578.7(b)
3. With the assistance of the Strategic Planning Committee develop a Continuum of Care plan consistent with 24 §CFR 578.7(c)

HMIS SYSTEM ADMINISTRATOR

The HMIS System Administrator is appointed to fulfill the following responsibilities:

SOFTWARE

1. Contract with the selected HMIS software operator (Vendor) for a period of one to five years. The contract is to include the cost of operating the HMIS and a minimum number of user licenses that meet the needs of Partner Agencies.
2. At the time of this document's writing, each HMIS User License costs $445 and the Vendor charges $137.50 per hour for work they must complete. Currently, Mendocino County HHSA incurs the operating cost of the HMIS, but reserves the right to revoke this voluntary payment with 30 day advance notice to the MCHSCoC Governing Board.
3. Serves as primary liaison between the HMIS software provider and the Partner Agencies.
4. Contracts with the HMIS software provider to administer and maintain central backup server operations including security procedures and daily system backup to prevent the loss of data.

TECHNICAL

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

Privacy and Security

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

The MCHSCoC Governing Board has appointed Mendocino County Health and Human Services Agency as its HMIS System Administrator.

HMIS LEAD AGENCY

The HMIS Lead Agency is appointed to fulfill the following responsibilities:

GENERAL

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

The MCHSCoC Governing Board has appointed Mendocino County Health and Human Services Agency as its HMIS Lead Agency.

DESIGNATING AN HMIS LEAD

The MCHSCoC Board reviews recommendations for the HMIS Lead once every 10 years. The HMIS/Performance Measurement Committee (HMIS/PMC) is responsible for providing recommendations for the CoC Board's vote. The HMIS/PMC completes an open competition at least once every 10 years to designate the HMIS Lead. The competition is posted by Request for Qualifications (RFQ) on the MCHSCoC website, and includes scoring criteria for applicants. The competition follows standard procurement protocol to seek, evaluate, and recommend an HMIS Lead. The HMIS/PMC meets to review applicants and votes on recommendations to the MCHSCoC Board. The MCHSCoC Board votes to approve the HMIS/PMC's recommendations for HMIS Lead. The HMIS Lead enters into a contract with the MCHSCoC. The MCHSCoC Board may also vote to re-procure the HMIS Lead agency if the current designated HMIS Lead does not fully implement the terms of their contract, does not provide satisfactory services, does not meet the below HMIS policies and procedures, or fails to meet HUD HMIS standards.

HMIS DAILY OPERATOR

The HMIS Daily Operator is appointed to fulfill the following responsibilities:

GENERAL

1. Informs MCHSCoC Governing Board of key HUD policies related to HMIS
2. Facilitates monthly MCHSCoC HMIS/PMC meetings to discuss system wide challenges
3. Attends HMIS meetings including HMIS End-Users Meetings and HMIS/PMC Meetings
4. Shares relevant/important information from HMIS meetings as needed
5. Coordinates the collection of data for HUD reports
6. Submits reports to HUD as required
7. Assists Partner Agencies with HUD or other funding reports and grant applications as needed
8. Promotes HMIS usage among all homeless service providers regardless of funding source
9. Provides all other reasonably expected activities regarding the day-to-day implementation and operation of HMIS

TECHNICAL

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

The MCHSCoC Governing Board has appointed Mendocino County Health and Human Services Agency as its HMIS Daily Operator.

MCHSCOC HMIS PERFORMANCE MEASUREMENT COMMITTEE

Another component of MCHSCoC's HMIS governance structure is the HMIS and Performance Measurement Committee (HMIS/PMC). Serving as an advisory group to the full MCHSCoC body, the HMIS/PMC makes critical recommendations about issues related to HMIS.

The HMIS/PMC's tasks include working with Mendocino County Continuum of Care (CoC) Lead Agency, and the HMIS Lead Agency/Grantee who also serves as the region's System Administrator and HMIS Daily Operator to:

1. Annually review this manual and any other HMIS policies and procedures required by HUD and provide recommendations to the full MCHSCoC body for final approval

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

The HMIS/PMC meetings occur monthly on the second Thursday of each month at 2:00 pm, hosted by HHSA in their office spaces as available. Teleconferencing is available for any persons unable to join in person The Mendocino County HHSA HOMe Team staffs the HMIS/PMC by scheduling the meetings, creating the agendas, facilitating the discussions, recording the minutes, and sharing recommendations with the full MCHSCoC body.

HMIS VENDOR SELECTION

Pursuant to MCHSCoC's Governance Charter, Mendocino County Homeless Services Continuum of Care Governing Board works with the MCHSCoC HMIS/PMC to designate a single software system for use as the MCHSCoC's HMIS. To designate a system, the following procurement process will be utilized:

1. Create a Scope of Work and Scoring Tool that contains details of the nature of the work needed to meet the needs of local Partner Agencies.
2. Issue a Request for Proposals/Qualifications to solicit responses from qualified HMIS vendors.
3. The MCHSCoC HMIS/PMC and HMIS Lead Agency will complete the Scoring Tool to evaluate the responses received and complete a recommendation of which software vendor to select.
4. The MCHSCoC Governing Board will make the final decision on which vendor to select.

SECTION 2: GENERAL OPERATING POLICIES AND PROCEDURES

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

HOW TO ADD AN AGENCY

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

1. Contact the HMIS Daily Operator
2. Read the following MCHSCoC documents:
   i. MCHSCoC Governance Charter
   ii. MCHSCoC HMIS Policies and Procedures Manual
3. Complete and submit the following forms to the HMIS Daily Operator:
   i. MCHSCoC New Project Agency Add Form
   ii. MCHSCoC HMIS Agency End User Agreement
   iii. MCHSCoC Interagency HMIS Data Sharing Agreement
4. Adopt either MCHSCoC's standard Privacy Policy (provided by the HMIS Lead Agency) or your own agency-specific Privacy Policy that satisfies all of the criteria listed in the 2004 HMIS Data and Technical Standards (see Section 4: HMIS Privacy and Security—Privacy Policy)
5. Post the Privacy Policy, along with the Privacy Notice and List of Participating Agencies (provided by the HMIS Lead Agency) at your intake desk(s) or comparable location(s)
6. If your agency maintains an agency website, post a link to the Privacy Policy on the homepage of the agency's website
7. Agree to ensure that hard copies of the following documents are available upon a client's request: HMIS End User Agreement (Appendix A), HMIS Privacy Notice (Appendix B), HMIS Privacy Policy (Appendix C), and HMIS Informed Consent & Release of Information Authorization Form (Appendix D), which includes a List of Participating Agencies
8. Agree to the cost and/or invoicing process as explained below:
   i. As the HMIS Lead Agency, Mendocino County Health and Human Services Agency (HHSA) oversees the cost/invoicing process. As such, Mendocino County Health and Human Services Agency (HHSA) does not have any associated fees to report at this time.

HOW TO ADD A NEW PROJECT

To add a new project to an already existing agency:

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

HOW TO ADD A USER

To add a user to an already existing agency:

1. Contact the HMIS Daily Operator
2. Read, complete, and submit the following forms to the HMIS Daily Operator for each new user:
   i. MCHSCoC HMIS User Account Request Form
   ii. MCHSCoC HMIS End User's Agreement
      (i) Please note this form requires the HMIS Participating Agency's Human Resources representative or Executive Director to sign the agreement, attesting that the agency conducted a criminal background check on the new user(s)
      (ii) The HMIS System Administrator will deny HMIS access to any potential new users who pleaded no contest or were convicted of any fraud (including identity theft) or stalking related felony crimes punishable by imprisonment of one year or more in any state (see Section 4: HMIS Privacy and Security—Background Check)
      (iii) The HMIS Daily Operator will forward the completed paperwork to by emailing hometeam@mendocinocounty.org and copying the new user(s)

HOW TO DISCONTINUE AN AGENCY

To discontinue an agency:

1. Send a message to the HMIS Daily Operator containing the following information:
   i. Reason for discontinuation
   ii. Official date agency wishes to discontinue use
      (i) Prior to contacting the HMIS Daily Operator, please ensure that your agency exited all active clients for each project(s). To do so, run a "Program Roster" report and select the "Active" status for each project(s)
2. The HMIS Daily Operator will then share the message with the HMIS Lead Agency
   i. Together, the agency, the HMIS Lead Agency, and the HMIS Daily Operator will determine the appropriate final payment amount and agree upon a final date for discontinued use

HOW TO DISCONTINUE A PROJECT

To discontinue a project:

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

HOW TO DISCONTINUE A USER

To discontinue a user:

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

HOW TO REQUEST TECHNICAL ASSISTANCE

To request technical assistance:

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

HOW TO REQUEST A MERGING OF TWO RECORDS

To request a merging of two records:

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

HOW TO REQUEST A PASSWORD RESET

To request a password reset:

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

HOW TO SUBMIT A DATA REQUEST

To submit a data request:

1. Send a message to the HMIS Daily Operator containing the following information:
   - i. Detailed summary of data request including:
     - (i) Purpose of the data request
     - (ii) Authority who approved this request
     - (iii) Requested report period
     - (iv) Preferred format for the data file
     - (v) Indicate if this is a system wide report, if not, what project types should be included e.g. only HUD-funded projects
     - (vi) Indicate what data elements need to be included
     - (vii) Indicate if you would like unduplicated data or all records collected
     - (viii) Due date
   - i. Call back number
   - ii. Please indicate if the issue is urgent e.g. need to submit a report by a particular deadline
     - (i)The HMIS Daily Operator will respond to your request within 48 hours of receipt unless it is a county-recognized holiday and/or the agency receives an out of office reply.

SECTION 3: HMIS DATA QUALITY PLAN

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

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

As stated at the beginning of this manual, MCHSCoC will review, revise, and re-ratify its HMIS Data Quality Plan annually upon a majority vote of all voting members present during the scheduled meeting. Prior to MCHSCoC's vote, the HMIS/PMC will recommend updates to the full MCHSCoC body according to HUD's latest HMIS Data Standards and Data Management Quality Program (DQMP) tools, and locally developed performance plans.

HMIS DATA STANDARDS

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

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

UNIVERSAL DATA ELEMENTS

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

The required Universal Data Elements include:

i. 3.1 Name
ii. 3.2 Social Security Number
iii. 3.3 Date of Birth
iv. 3.4 Race
v. 3.5 Ethnicity
vi. 3.6 Gender
vii. 3.7 Veteran Status
viii. 3.8 Disabling Condition
ix. 3.9 Residence Prior to Project Entry
x. 3.10 Project Entry Date
xi. 3.11 Project Exit Date
xii. 3.12 Destination

xiii. 3.13 Personal ID
xiv. 3.14 Household ID
xv. 3.15 Relationship to Head of Household
xvi. 3.16 Client Location
xvii. 3.17 Length of Time on Street, in an Emergency Shelter or Safe Haven

PROGRAM-SPECIFIC DATA ELEMENTS

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

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

The required Program-Specific Data Elements include:

i. 4.1 Housing Status
ii. 4.2 Income and Sources
iii. 4.3 Non-Cash Benefits
iv. 4.4 Health Insurance
v. 4.5 Physical Disability
vi. 4.6 Developmental Disability
vii. 4.7 Chronic Health Condition
viii. 4.8 HIV/AIDS
ix. 4.9 Mental Health Condition
x. 4.10 Substance Abuse
xi. 4.11 Domestic Violence
xii. 4.12 Contact
xiii. 4.13 Date of Engagement
xiv. 4.14 Services Provided
xv. 4.15 Financial Assistance Provided
xvi. 4.16 Referrals Provided
xvii. 4.17 Residential Move-In Date
xviii. 4.18 Housing Assessment Disposition
xix. 4.19 Housing Assessment at Exit

PROJECT DESCRIPTOR DATA ELEMENTS

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

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

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

The required Project Descriptor Data Elements include:

i. 2.1 Organization Identifiers
ii. 2.2 Project Identifiers
iii. 2.3 Continuum of Care Code
iv. 2.4 Project Type
v. 2.5 Method for Tracking Emergency Shelter
vi. 2.6 Federal Partner Funding Sources
vii. 2.7 Bed and Unit Inventory Information
viii. 2.8 Site Information – Optional
ix. 2.9 Target Population

GOALS

TIMELINESS

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

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

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

i. Entry data should be entered into MCHSCoC HMIS as soon as possible but no later than 72 hours after client/household entered the project.
ii. Exit data should be entered as soon as possible but not later than 72 hours after the client/household exited the project.
iii. Shelter exits (emergency and transitional housing programs only)
    (i) Client/Household must be exited in MCHSCoC HMIS within 72 hours of program exit.
    (ii) Night-by-Night Shelter Tracking Method
        - MCHSCoC Emergency Shelters utilizing night-by-night shelter tracking method(s) shall use ninety (90) days with no content as the extending period of time after which a client is exited from the shelter project.

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

COMPLETENESS

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

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

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

BED/UNIT UTILIZATION RATES

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

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

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

TABLE 1 REASON FOR LEAVING DEFINITIONS AND BEST PRACTICES

- The table below is a guide to assist HMIS End Users in utilizing the most appropriate 'Reason for Leaving' when entering client exit data:

Reason for Leaving	Description
Completed Program	Client was successful and completed the program. Successful referral made. Client chose to end enrollment on good terms and does not fit match any other reason.
Criminal Activity/Property Destruction	Any criminal activity or violent behavior that may result in police involvement or safety concerns. Involuntarily left housing project due to property destruction.
Death	Client has passed away.
Disagreement with Rules/Person	A disagreement with a program rule or person that creates a significant obstacle or barrier to an individual's stay in a program.
Left for Housing before Completed	Client located housing without project assistance, in or out of county.
Needs Could Not Be Met By Project	Project couldn't meet specific client need(s). Client moved out of CoC coverage area.
Non-Compliance with Project	Non-compliance with project rules where exit is necessary.
Non-Payment of Rent/Occupancy Charge	Client was unable to follow program guidelines pertaining to rent or fees.
Max Time Allowed in Project	Project term limits have been exhausted.

As a continuum, we want to avoid these answers. They don't offer meaningful client data for reports or decision making.	
Unknown/Disappeared	No contact with client for a number of days dictated by HMIS or agency policy.
Other	Other should only be used in very unique situations and always requires a note explaining the reason. Partner with HMIS Administrator before using Other

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

BED COVERAGE RATES

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

This is an important rate to calculate to ensure that MCHSCoC meets HUD's minimum threshold of at least 50% to be eligible for the Longitudinal Systems Analysis (LSA). Without meeting the 50% threshold, HUD is unable to project estimates for non-HMIS projects with reasonable statistical confidence.

SERVICE-VOLUME COVERAGE RATES

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

This is an important rate to calculate to ensure that MCHSCoC meets HUD's minimum threshold of at least 50% to be eligible for the Longitudinal Systems Analysis (LSA). Without meeting the 50% threshold, HUD is unable to project estimates for non-HMIS projects with reasonable statistical confidence.

OTHER IMPORTANT DATA QUALITY PRACTICES

MCHSCoC's HMIS Data Quality Management Plan (DQMP) will be developed upon the tool's release by HUD, and will be revised annually in April. The DQMP revision process will include an annual verification of Project Descriptor Data Elements and residential housing projects, as well as establishing local standards regarding accuracy.

TABLE 2 AGENCY SITE ADMINISTARTORS TASK LIST

1. Run a MCHSCoC HMIS report for each program. Review number of open cases to verify	Monthly

that they equal the number of actual open cases. • Exit cases that should be closed. • Enter cases that should be open.	
2. Pull 10% pf paper files and compare with MCHSCoC HMIS data to verify that data is accurate.	Monthly
3. If an overnight shelter, then check Resident/Bed List to verify accuracy against paper shelter list.	Weekly
4. If shelter or transitional housing program, check Resident/Bed List to verify that number of open cases on MCHSCoC HMIS report equals the number of individuals and households on Resident/Bed List.	Monthly
5. Issue monthly Data Quality Assurance Report to agency Executive Director on status of quality assurance monitoring check.	Monthly

ANNUAL VERIFICATIONS

Every year prior to the Longitudinal Systems Analysis (LSA) and Housing Inventory Count (HIC), the HMIS Daily Operator will request agencies to verify their Project Descriptor Data Elements (see Section 3: HMIS Data Quality Plan—Project Descriptor Data Elements) as well as their inventory of residential housing projects.

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

ACCURACY

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

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

Some important things to note regarding accuracy include:

i. All Universal Data Elements and Program Specific Data Elements must be obtained from each adult and unaccompanied youth who apply for services

ii. Most Universal Data Elements are also required for children age 17 years and under

iii. Most Universal Data Elements and Program-Specific Data Elements include a "Client Doesn't Know" or "Client Refused" response category. HUD considers these valid responses if the client does not know or the client refuses to respond to the question. It is not the intention of HUD, or any other funders who require HMIS usage, to have agencies deny clients assistance if they refuse or are unable to supply the information. However, some information may be required by projects or public or private funders to determine eligibility for housing or services, or to assess needed services.

iv. Agencies should not use the “Client Doesn’t Know” or “Client Refused” responses to indicate that the case manager or data entry staff member does not know the client’s response

v. Since MCHSCoC’s HMIS requires a response to all data fields before saving a record, the agency should use the “Data not collected” response to indicate missing data

MONITORING

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

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

MONITORING ROLES AND RESPONSIBILITIES

Mendocino County Health and Human Services Agency (HHSA) fulfills the role of HMIS System Administrator, HMIS Lead/Grantee, and the Daily Operator.

HMIS System Administrator

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

MCHSCoC HMIS Lead/Grantee

The MCHSCoC HMIS Lead/Grantee is responsible for reviewing each project’s data quality on a quarterly basis, and correcting data entry errors for each project within HMIS. The HMIS Lead/Grantee will work to identify issues that do not comply with the agreed-upon goals and benchmarks. Based from the HMIS Lead/Grantee assessment, the HMIS Daily Operator will offer individualized support and develop specialized trainings as necessary.

HMIS Daily Operator

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

MONITORING SCHEDULE

As stated above, the HMIS/PMC meetings occur monthly on the second Thursday of each month at 2:00 pm, hosted by HHSA in their office spaces as available. Teleconferencing is available for any persons unable to join in person the Mendocino County HHSA HOMe Team staffs the HMIS/PMC by scheduling the meetings, creating the agendas, facilitating the discussions, recording the minutes, and sharing recommendations with the full MCHSCoC body.

SECTION 4: HMIS PRIVACY AND SECURITY PLAN

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

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

As stated at the beginning of this manual, MCHSCoC will review, revise, and re-ratify the HMIS Privacy and Security Plan annually upon a majority vote of all voting members present during the scheduled meeting. Prior to MCHSCoC's vote, the MCHSCoC HMIS/PMC will recommend updates to the full MCHSCoC body according to HUD's latest HMIS standards. It is important to note that the Plan complies with HUD's 2004 HMIS Data and Technical Standards Final Notice3 as well as state and local laws regulating the confidentiality of personal information. Yet, at the time of writing this Plan, HUD has not yet released a final notice regarding HMIS security. Given this, the Plan contains preliminary security safeguards; however, MCHSCoC anticipates updating the safeguards upon receiving final guidance from HUD.

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

HMIS DATA AND TECHNICAL STANDARDS

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

PRIVACY POLICY

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

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

Additional Information about the Privacy Policy

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

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

Partner Agencies may use and disclose PPI to:

i. Verify eligibility for services
ii. Provide clients with and/or refer clients to services that meet their needs
iii. Manage and evaluate the performance of programs
iv. Report about program operations and outcomes to funders and/or apply for additional funding to support agency programs
v. Collaborate with other local agencies to improve service coordination, reduce gaps in services, and develop community-wide strategic plans to address basic human needs
vi. Participate in research projects to better understand the needs of people served

Partner Agencies may also be required to disclose PPI for the following reasons:

i. When the law requires it
ii. When necessary to prevent or respond to a serious and imminent threat to health or safety
iii. When a judge, law enforcement or administrative agency orders it

Partner Agencies are obligated to limit disclosures of PPI to the minimum necessary to accomplish the purpose of the disclosure. Uses and disclosures of PPI not described above may only be made with a client's written consent. Clients have the right to revoke consent at any time by submitting a request in writing.

Clients also have the right to request in writing:

i. A copy of all PPI collected
ii. An amendment to any PPI used to make decisions about the client's care and services (this request may be denied at the discretion of the agency, but the client's request should be noted in the project records)
iii. An account of all disclosures of client PPI
iv. Restrictions on the type of information disclosed to outside partners
v. A current copy of the agency's Privacy Policy

Partner Agencies may reserve the right to refuse a client's request for inspection or copying of PPI in the following circumstances:

i. Information compiled in reasonable anticipation of litigation or comparable proceedings
ii. The record includes information about another individual (other than a health care or homeless provider)

iii. The information was obtained under a promise of confidentiality (other than a promise from a health care or homeless provider) and a disclosure would reveal the source of the information
iv. The Partner Agency believes that disclosure of the information would be reasonably likely to endanger the life or physical safety of any individual

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

All individuals with access to PPI are required to complete formal training in privacy requirements at least annually.

Partner Agencies can amend their Privacy Policies at any time. Amendments may affect information obtained by the agency before the date of the change. An amendment to the Privacy Policy regarding use or disclosure will be effective with respect to information processed before the amendment, unless otherwise stated. The agency must make available a record of all amendments to the Privacy Policy upon a client's request.

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

PRIVACY NOTICE

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

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

LIST OF PARTICIPATING AGENCIES

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

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

INFORMED CONSENT AND RELEASE OF INFORMATION AUTHORIZATION

The Informed Consent and Release of Information Authorization must be signed by all adult clients and unaccompanied youth. This gives the client the opportunity to refuse the sharing of his or her information to other agencies within the system. MCHSCoC requires client signatures prior to inputting their information in HMIS. MCHSCoC also requires agencies to update Informed Consent and Release of Information Authorization forms every five years.

PRIVACY AND SECURITY SAFEGUARDS

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

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

PHYSICAL SAFEGUARDS

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

Computer Location

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

Printer Location

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

Monitor

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

Mobile Device

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

TECHNICAL SAFEGUARDS

Workstation Security

To promote the security of HMIS and the confidentiality of the data contained therein, MCHSCoC will only allow access to HMIS through approved workstations. To ensure compliance, the HMIS System Administrator will enlist the use of an IP Address Whitelist or another suitably secure method to identify approved workstations, in compliance with Public Access baseline requirement in the HUD Data Standards (4.3.1 System Security). Users will be required to submit the IP Address of their workstation to the HMIS System Administrator to be registered into the system and will notify the System Administrator should this number need to be changed.

Establishing HMIS User IDs and Access Levels

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

User Authentication

i. Usernames are individual and passwords are confidential. No individual should ever use or allow use of a username that is not assigned to that individual and passwords should never be shared or communicated in any format
ii. The system requires users to change temporary passwords upon first use. Passwords must be a minimum of six (6) characters long and must contain a combination of upper case and lower case letters, a number, and a symbol
iii. End users will be prompted by the software to change their password every ninety (90) days
iv. End Users must immediately notify the HMIS System Administrator if they have reason to believe that someone else has gained access to their password
v. Three consecutive unsuccessful attempts to login will disable the username until the HMIS Daily Operator resets the password
vi. End users must log out from the HMIS application and either lock or log off their respective workstation if they leave. If the user logged into HMIS and the period of inactivity in HMIS exceeds 45minutes, the user will be logged off the HMIS system automatically

Rescinding User Access

i. The Partner Agency will notify the HMIS System Administrator at least 24-hours if an end user no longer requires access to perform his or her assigned duties due to a change of job duties or termination of employment.
ii. The HMIS System Administrator reserves the right to terminate end user licenses that are inactive for 60 days or more
iii. The HMIS System Administrator will attempt to contact the Partner Agency for the end user in question prior to termination of the user’s license
iv. In the event of suspected or demonstrated noncompliance by an end user with the HMIS End User Agreement or any other HMIS plans, forms, standards or governance documents, the Partner Agency Security Officer must notify the HMIS System Administrator to deactivate the user’s license while the Partner Agency Security Office conducts an internal agency investigation

v. Any user found to have misappropriated client data (identity theft, releasing personal client data to any unauthorized party) will have his or her HMIS privileges revoked

vi. MCHSCoC is empowered to permanently revoke a Partner Agency's access to HMIS for substantiated noncompliance with the provisions of this Plan that resulted in a release of PPI

Disposing Electronic, Hardcopies, Etc.

i. Computer: All technology equipment (including computers, printers, copiers and fax machines) used to access HMIS and which will no longer be used to access HMIS will have their hard drives reformatted multiple times. If the device is now non-functional, it must have the hard drive pulled, destroyed and disposed of in a secure fashion

ii. Hardcopies: For paper records, shredding, burning, pulping, or pulverizing the records so that PPI is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed

iii. Mobile Devices: Use software tools that will thoroughly delete/wipe all information on the device and return it to the original factory state before discarding or reusing the device

Other Technical Safeguards

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

ii. MCHSCoC requires that each HMIS Partner Agency develop and implement procedures that will prevent unauthorized users from connecting to private agency networks

III. Unencrypted PPI may not be stored or transmitted in any fashion—including sending file attachments by email or downloading reports including PPI to a flash drive, to the End User's desktop or to an agency shared drive. All downloaded files containing PPI must be deleted from the workstation temporary files and the "Recycling Bin" emptied before the End User leaves the workstation

DISASTER RECOVERY POLICY

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

i. Be aware of and be trained to complete any tasks or procedures for which they are responsible in the event of a disaster

ii. Have a plan for restoring local computing capabilities and internet connectivity for the HMIS System Administrator's facilities

iii. Maintain a readily accessible list of account numbers and contact information for its internet service provider, support contracts, and equipment warranties

iv. Maintain a list of the computer and network equipment required to restore minimal access to HMIS and to continue providing services to HMIS Partner Agencies

v. Maintain documentation of the configuration settings required to restore local user accounts and internet access

WORKFORCE SECURITY POLICY

HMIS Access to Active Clients

MCHSCoC has an open HMIS system and most HMIS Users have access to client's current or past history from other agencies. With the goal of protecting the security and integrity of the HMIS system and safeguarding the personal information contained therein, MCHSCoC will no longer give HMIS access to individuals who are actively receiving services from any HMIS partner agency with an active record in the MCHSCoC HMIS.

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

BACKGROUND CHECK POLICY

HMIS End User Background Check Requirements

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

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

i. Bank Fraud: To engage in an act or pattern of activity where the purpose is to defraud a bank of funds
ii. Blackmail: A demand for money or other consideration under threat to do bodily harm, to injure property, to accuse of a crime, or to expose secrets
iii. Bribery: When an individual offers money, goods, services, information or anything else of value with intent to influence the actions, opinions, or decisions of the taker. You may be charged with bribery whether you offer the bribe or accept it
iv. Computer fraud: Where computer hackers steal information sources contained on computers such as: bank information, credit cards, and proprietary information
v. Credit Card Fraud: The unauthorized use of a credit card to obtain goods of value
vi. Extortion: Occurs when one person illegally obtains property from another by actual or threatened force, fear, or violence, or under cover of official right
vii. Forgery: When a person passes a false or worthless instrument such as a check or counterfeit security with the intent to defraud or injure the recipient
viii. Health Care Fraud: Where an unlicensed health care provider provides services under the guise of being licensed and obtains monetary benefit for the service
ix. Larceny/Theft: When a person wrongfully takes another person's money or property with the intent to appropriate, convert or steal it
x. Money Laundering: The investment or transfer of money from racketeering, drug transactions or other embezzlement schemes so that it appears that its original source either cannot be traced or is legitimate
xi. Telemarketing Fraud: Actors operate out of boiler rooms and place telephone calls to residences and corporations where the actor requests a donation to an alleged charitable organization or where the actor requests money up front or a credit card number up front, and does not use the donation for the stated purpose

xii. Welfare Fraud: To engage in an act or acts where the purpose is to obtain benefits (i.e. Public Assistance, Food Stamps, or Medicaid) from the State or Federal Government

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

MONITORING

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

ROLES AND RESPONSIBILITIES

HMIS System Administrator

As the HMIS System Administrator, Mendocino County Health and Human Services Agency (HHSA):

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

HMIS Daily Operator

As the HMIS Daily Operator, Mendocino County Health and Human Services Agency (HHSA):

i. Provides technical assistance to agencies and users who need assistance complying with MCHSCoC's Privacy and Security Plan

MCHSCoC HMIS Performance Measurement Committee

As an advisory group to the full MCHSCoC body, the HMIS/PMC:

i. Makes annual recommendations to the full MCHSCoC body regarding revisions to the Plan
ii. Monitors agencies and users to ensure adherence to the roles and responsibilities delineated within MCHSCoC's Privacy and Security Plan
iii. Develops technical assistance, action and/or compliance plans for agencies that the HMIS/PMC finds to be in violation of MCHSCoC's Privacy and Security Plan

HMIS Partner Agency

The HMIS Partner Agency is responsible for ensuring the following standards are upheld by their staff:

i. Prevents degradation of the HMIS resulting from viruses, intrusion, or other factors within the agency's control and prevents the inadvertent release of confidential client-specific information through physical, electronic or visual access to user workstations
ii. Ensures the agency meets the privacy and security requirements detailed in the HUD HMIS Data and Technical Standards
iii. Adopts and upholds a Privacy Policy, which meets or exceeds all minimum standards including substance use providers covered by 24 CFR Part 2, HIPPA covered agencies

(i) Modifications to MCHSCoC's standard Privacy Policy must be approved by the MCHSCoC HMIS/PMC

iv. Ensures that all clients are aware of the adopted Privacy Policy and have access to it o If the agency has a website, the agency must publish the Privacy Policy on their website
v. Makes reasonable accommodations for persons with disabilities, language barriers, or education barriers
vi. Ensures that anyone working with clients covered by the Privacy Policy can meet the user responsibilities
vii. Designates at least one Security Officer that has been trained to technologically uphold the adopted Privacy Policy

HMIS End User

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

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

Partner Agency Security Officer

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

i. May be the HMIS System Administrator or another employee, volunteer or contractor designated by MCHSCoC who has completed HMIS Privacy and Security training and is adequately skilled to assess HMIS security compliance
ii. Assesses security measures in place prior to establishing access to HMIS for a new Agency
iii. Reviews and maintains file of Partner Agency annual compliance certification checklists
iv. Conducts annual security audit of all Partner Agencies
v. Partner Agency Security Officer will confirm that any workstation accessing HMIS shall have antivirus software with current virus definitions (updated at minimum every 24 hours) and frequent full system scans (at minimum weekly)
vi. Partner Agency Security Officer will confirm that any workstation accessing HMIS has and uses a hardware or software firewall; either on the workstation itself if it accesses the internet through a modem or on the central server if the workstation(s) accesses the internet through the server

Upon request, the HMIS Lead Agency may be available to provide Security support to Partner Agencies who do not have the staff capacity or resources to fulfill the duties assigned to the Partner Agency Security Officer.

HMIS Lead Agency Security Officer

The HMIS Lead Agency will appoint an HMIS Lead Agency Security Officer who will provide support to HMIS Participating Agencies to comply with HMIS Privacy and Security policies.

i. May be the Partner Agency HMIS Agency Administrator or another Partner Agency employee, volunteer or contractor who has completed HMIS Privacy and Security training and is adequately skilled to assess HMIS security compliance,

ii. Conducts a security audit for any workstation that will be used for HMIS purposes
    - (i) No less than semiannually for all agency HMIS workstations
    - (ii) Prior to issuing a User ID to a new HMIS End User
    - (iii) Any time an existing user moves to a new workstation

iii. Continually ensures each workstation within the Partner Agency used for HMIS data collection or entry is adequately protected by a firewall and antivirus software (per Technical Safeguards–Workstation Security)

iv. Completes the semiannual Compliance Certification Checklist, and forwards the Checklist to the Lead Security Officer

NEW HMIS PARTNER AGENCY SITE SECURITY ASSESSMENT

Prior to establishing access to HMIS for a new Partner Agency, the Lead Security Officer will assess the security measures in place at the Partner Agency to protect client data (see Technical Safeguards–Workstation Security). The Lead Security Officer or other HMIS System Administrator will meet with the Partner Agency Executive Director (or executive-level designee) and Partner Agency Security Officer to review the Partner Agency's information security protocols prior to countersigning the HMIS Memorandum of Understanding. This security review shall in no way reduce the Partner Agency's responsibility for information security, which is the full and complete responsibility of the Partner Agency, its Executive Director, and its HMIS Agency Security Officer.

SEMIANNUAL PARTNER AGENCY SELF-AUDITS

i. The Partner Agency Security Officer will use the Compliance Certification Checklist to conduct semiannually security audits of all Partner Agency HMIS End User workstations.

ii. The Partner Agency Security Officer will audit for inappropriate remote access by End-Users by associating User login date/times with employee time sheets. End Users must certify that they will not remotely access HMIS from a workstation (i.e. personal computer) that is not subject to the Partner Agency Security Officer's regular audits.

iii. If areas are identified that require action due to noncompliance with these standards or any element of the MCHSCoC HMIS Policies and Procedures, the Partner Agency Security Officer will note these on the Checklist, and the Partner Agency Security Officer and/or HMIS Agency Administrator will work to resolve the action item(s) within fifteen (15) days

iv. Any Checklist that includes one or more findings of noncompliance and/or action items will not be considered complete until all action items have been resolved. The findings, action items, and resolution summary must be reviewed and signed by the Agency's Executive Director or other empowered officer prior to being forwarded to the Lead Security Officer

v. The Partner Agency Security Officer must turn in a copy of the Checklist to the Lead Security Officer on a semiannual basis

ANNUAL SECURITY AUDITS

i. The HMIS Lead Agency Security Officer will schedule the annual security audit in advance with the Partner Agency Security Officer

ii. The HMIS Lead Agency Security Officer will use the Compliance Certification Checklist to conduct security audits

iii. The HMIS Lead Agency Security Officer must randomly audit at least 10% of the workstations used for HMIS data entry for each HMIS Partner Agency. In the event that an agency has more than one project site, at least one workstation per project site must be audited

iv. If areas are identified that require action due to noncompliance with these standards or any element of the MCHSCoC HMIS Policies and Procedures, the Lead Security Officer will note these on the Checklist, and the Partner Agency Security Officer and/or HMIS Agency Administrator will work to resolve the action item(s) within fifteen (15) days

v. Any Checklist that includes one or more findings of noncompliance and/or action items will not be considered complete until all action items have been resolved and the findings, action items, and resolution summary has been reviewed and signed by the Agency's Executive Director or other empowered officer and forwarded to the HMIS Lead Agency Security Officer.

REPORTING SECURITY INCIDENTS

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

i. Any user who becomes aware of or suspects a compromise in HMIS security and/or client privacy must immediately report the concern to their agency's Security Officer.

ii. In the event of a suspected security or privacy concern, the agency Security Officer should complete an internal investigation

iii. If the suspected security or privacy concern resulted from a user's suspected or demonstrated noncompliance with the HMIS End User Agreement, the Security Officer should have the HMIS System Administrator deactivate the user's account until the internal investigation has been completed

iv. Following the internal investigation, the Security Officer should notify the Lead Security Officer of any substantiated incidents that may have compromised HMIS system security and/or client privacy whether or not a release of client PPI is definitively known to have occurred

v. If the security or privacy concern resulted from demonstrated noncompliance by a user with a signed HMIS End User Agreement, the Lead Security Officer reserves the right to permanently deactivate the user account for the user in question

vi. Within one business day after the Lead Security Officer receives notice of the security or privacy concern, the Lead Security Officer and Partner Agency Security Officer will jointly establish an action plan to analyze the source of the security or privacy concern and actively prevent such future concerns

vii. The user or agency must implement the action plan as soon as possible, and the total term of the plan must not exceed thirty (30) days

viii. If the user or agency is not able to meet the terms of the action plan within the time allotted, the HMIS System Administrator, in consultation with the full MCHSCoC body, may elect to terminate the agency's access to HMIS

ix. The agency may appeal to MCHSCoC for reinstatement to HMIS following completion of the requirements of the action plan

x. In the event of a substantiated release of PPI in noncompliance with the provisions of the MCHSCoC Privacy and Security Plan, this manual, or the Privacy Policy, the Security Officer will make a reasonable attempt to notify all impacted individual(s)

xi. The Lead Security Officer must approve of the method of notification and the agency Security Officer must provide the Lead Security Officer with evidence of the agency's notification attempt(s)

xii. If the Lead Security Officer is not satisfied with the agency's efforts to notify impacted individuals, the Lead Security Officer will attempt to notify impacted individuals at the agency's expense

xiii. The HMIS System Administrator will notify MCHSCoC of any substantiated release of PPI in noncompliance with the provisions of MCHSCoC's Privacy and Security Plan, this manual, or the Privacy Policy

xiv. The HMIS System Administrator will maintain a record of all substantiated releases of PPI in noncompliance with the provisions of MCHSCoC's Privacy and Security Plan, this manual, or the Privacy Policy for 7 years

xv. MCHSCoC reserves the right to permanently revoke an agency's access to HMIS for substantiated noncompliance with the provisions of MCHSCoC's Privacy and Security Plan, this manual, or the Privacy Policy that resulted in a release of PPI

APPENDIX A: HMIS End User Agreement

Mendocino County Homeless Services Continuum of Care
Homeless Management Information System (HMIS) End User Agreement

This agreement applies to all individuals working at agencies participating in the Homeless Management Information System (HMIS) implemented by the Mendocino County Homeless Services Continuum of Care (MCHSCoC) through the HMIS Lead agency of the Mendocino County Health and Human Services Agency (HHSA).

All members of the continuum will act in good faith to the continuum and its mission. **The mission of the MCHSCoC is to *create an effective continuum of outreach, housing and support services for the homeless of Mendocino County*.** All members will use professional integrity, care, skill, and diligence when carrying out any acts affiliated with the continuum. All members will use the highest standards of integrity, honesty, ethics and fairness when carrying out any and all duties associated with the MCHSCoC.

Individuals working in HMIS will have access to confidential information regarding clients and services. All confidential information obtained will be held in the highest confidence by individuals. Agencies will reassure clients that confidential information will only be used as necessary, in the interest of client progress and program compliance. Confidential information will not be shared or used outside of the parameters of the Release of Information granted by the client.

Individuals should report any violations of this Confidentiality Agreement to the HMIS Lead Agency. The HMIS Lead Agency will investigate all reports and take appropriate disciplinary action up to and including barring Agencies from participation in the MCHSCoC for a specified period of time, and funding associated with that participation.

Security for data maintained in HMIS depends on a secure computing environment. Computer security is adapted from relevant provisions of the Department of Housing and Urban Development's (HUD) "Homeless Management Information Systems (HMIS) Data and Technical Standards Notice" (see https://www.hudexchange.info/hmis/hmis-data-and-technical-standards/). Agencies are encouraged to directly consult that document for complete documentation of HUD's standards relating to HMIS. Agencies will allow access to HMIS only from computers that are:

(i) Physically present on Agency's premises:
(ii) Owned by Agency; or
(iii) Approved by Agency for the purpose of accessing and working with HMIS; and
(iv) protected from viruses by commercially available virus protection software,
(v) protected with a software or hardware firewall,
(vi) maintained to insure that the computer operating system running the computer used for the HMIS is kept up to date in terms of security and other operating system patches, updates, and fixes,
(vii) Accessed through web browsers with 128-bit encryption (e.g., Internet Explorer, version 10.0). Some browsers have the capacity to remember passwords, so that the user does not need to type in the password when returning to password-protected sites. This default shall NOT be used with respect to HMIS; the end-user is expected to physically enter the password each time he or she logs on to the system,
(viii) Staffed at all times when in public areas. When computers are not in use and staff are not present, steps should be taken to ensure that the computers and data are secure and not publicly accessible. These steps should minimally include: Logging off the data entry system, physically locking the computer in a secure area, or shutting down the computer entirely.

Passwords: Member agencies will permit access to HMIS only with use of a user ID and password which the user may not share with others. Written information pertaining to user access (e.g. username and password) shall not be stored or displayed in any publicly accessible location. Passwords shall be at least eight characters long and meet industry standard complexity requirements, including, but not limited to, the use of at least one of each of the following kinds of characters in the passwords: upper and lower-case letters, and numbers and symbols. Passwords shall not be, or include, the username, or the HMIS name. In addition, passwords should not consist entirely of any word found in the common dictionary or any of the above spelled backwards. The use of default passwords on initial entry into the HMIS application is allowed so long as the application requires that the default password be changed on first use. Passwords and user names shall be consistent with guidelines issued from time to time by HUD.

Member agencies will permit access to HMIS only after the authorized user receives appropriate confidentiality training. Agencies will also conduct ongoing basic confidentiality training for all persons with access to HMIS and will train all persons who may receive information produced from HMIS on the confidentiality of such information. Member agencies are responsible for ensuring their current and future employees are trained regarding this specific HMIS confidentiality agreement. Member agencies will be accountable for employee actions. Member agencies are responsible for notifying the HMIS Administrator when new employees require access to HMIS. Member agencies are responsible for notifying the HMIS Administrator when employees leave employment with the agency so access to HMIS can be removed.

*Note- HMIS End users with active access can log into HMIS from any device with internet; therefore, it is imperative to notify the HMIS Administrator immediately following the employee's departure from the agency.

Each new HMIS participant agency, individual employees, and the Mendocino County Homeless Services Coordinator, or her/his representative, will together review this confidentiality agreement. After review two copies of the agreement will be signed and dated by both the individual and the coordinator, or her/his representative. Individuals will keep one signed, dated original for their record and one original will be kept with the oversight agency, or Mendocino County Health and Human Services Agency.

ACKNOWLEDGMENT OF HMIS END USER AGREEMENT

I have received, read and understand the HMIS End User Agreement for the Mendocino County Homeless Services Continuum of Care Homeless Management Information System.

Name of Agency:	
Printed Name of Individual:	
Individual Signature:	Date:
Title:	
Work Phone:	Work Email:
Printed Name of Agency Administrator/Director:	
Signature:	Date:
Agency Admin or Director is responsible for notifying the HMIS Administrator when new employees require access to HMIS and when employees leave employment with the agency so access to HMIS can be removed.	
Printed Name of HMIS Lead Agency Administrator:	
Signature:	Date:

Appendix B: HMIS Privacy Notice

Mendocino County Continuum of Care

HOMELESS MANAGEMENT INFORMATION SYSTEM (HMIS)

PRIVACY NOTICE

We collect personal information directly from you for reasons that are discussed in our Privacy Policy. We may be required to collect some personal information by law or by organizations that give us money to operate this program.

Other personal information that we collect is important to run our programs, to improve services for individuals who are experiencing homelessness, and to better understand their needs.

This policy may be amended at any time, which may include amendments that may affect information obtained before the date of the change. An amendment to the privacy notice regarding use or disclosure will be effective with respect to information processed before the amendment, unless otherwise stated.

We are partnering with the Veterans Administration.

We only collect information that we consider to be appropriate.

Appendix C: HMIS Privacy Policy

I. HMIS PRIVACY POLICY OVERVIEW

A. This notice describes the Homeless Management Information System (HMIS) privacy policy and practices of Mendocino County Continuum of Care. Our main office is located at 747 S. State Street, Ukiah, CA 95482.

B. The policy and practices in this notice covers the collection, use, and maintenance of protected personal information for persons served by Mendocino County Continuum of Care, as an organization affiliated with the Homeless and Poverty Action Coalition (HPAC). If this agency is a covered entity under HIPAA, you may have additional rights regarding your protected health information and these rights will be described to you in the agency's Policy of Privacy Practices under HIPAA.

C. Personally identifiable information or protected personal information (PPI) is any information we maintain about a client that:

1. Allows identification of an individual directly or indirectly;
2. Can be manipulated by a reasonably foreseeable method to identify a specific individual; or
3. Can be linked with other available information to identify a specific client.

D. We adopted this policy because the U.S. Department of Housing and Urban Development (HUD) issued standards for HMIS systems. We intend our policy and practices to be consistent with those standards. See 69 Federal Register 45888 (July 30, 2004).

E. This notice informs our clients, our staff, and others how we process personal information. We follow the policy and practices described in this notice.

F. We may amend this notice and our policy or practices at any time. Amendments may affect personal information that we obtained before the effective date of the amendment.

1. Amendments to this privacy policy will be approved by the HMIS System Administrator and HMIS Lead Agency.

G. We give a written copy of this privacy policy to any individual who asks.

II. HOW AND WHY WE COLLECT PERSONAL INFORMATION

A. We collect PPI only when appropriate to provide services or for another specific purpose of our agency or when required by law. We may collect information to:

1. Provide or coordinate services to clients;
2. Produce aggregate-level reports regarding use of services;
3. Track individual project-level outcomes;
4. Identify unfilled service needs and plan for the provision of new services;
5. Conduct research for consulting and/or educational purposes;

6. For functions related to payment or reimbursement from others for the services we provide;
7. To operate our organization, including administrative functions such as legal, audits, personnel, oversight, and management functions; and
8. Accomplish any and all other purposes deemed appropriate by HPAC.

B. We only use lawful and fair means to collect personal information.

C. We normally collect personal information with the knowledge or consent of our clients. If you seek our assistance and provide us with personal information, we assume that you consent to the collection of information as described in this notice.

D. We may also collect information about you from:

1. Individuals who are with you;
2. Other private organizations that provide services; All HMIS participating agencies.
3. Government agencies; US Department of Veteran Affairs, Mendocino County HHSA, City of Ukiah, City of Willits, City of Fort Bragg, and
4. Telephone directories and other published sources.

E. We share this data with three agencies to manage all personal information we record about our clients:

1. Mendocino County Continuum of Care;
2. HMIS Lead Agency;
3. Coordinated Entry Lead Agency; and
4. California State Homeless Data Integration System (HDIS).

F. We post a Consumer Notice at our intake desk or other location explaining the reasons we ask for personal information. The Consumer Notice reads:

We collect personal information directly from you for reasons that are discussed in our Privacy Policy. We may be required to collect some personal information by law or by organizations that give us money to operate this program.

Other personal information that we collect is important to run our programs, to improve services for individuals who are experiencing homelessness, and to better understand their needs.

This policy may be amended at any time, which may include amendments that may affect information obtained before the date of the change. An amendment to the privacy notice regarding use or disclosure will be effective with respect to information processed before the amendment, unless otherwise stated.

We are partnering with the Veterans Administration.

We only collect information that we consider to be appropriate.

III. HOW WE USE AND DISCLOSE PERSONAL INFORMATION

A. We use or disclose personal information for activities described in this part of the policy. We may or may not make any of these uses or disclosures with your information. We assume that you consent to the use or disclosure of your personal information for the purposes described below and for other uses and disclosures that we determine to be compatible with these uses or disclosures:

1. To provide or coordinate services to individuals; data may be shared with other HMIS participating agencies;
2. For functions related to payment or reimbursement for services;
3. To carry out administrative functions such as legal, audits, personnel, oversight, and management functions;
4. To create de-identified (anonymous) information that can be used for research and statistical purposes without identifying clients
5. When required by law to the extent that use or disclosure complies with and is limited to the requirements of the law;
6. To avert a serious threat to health or safety if;
   a. We believe that the use or disclosure is necessary to prevent or lessen a serious imminent threat to the health or safety of an individual or the public; and
   b. The use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat.
7. To report about an individual we reasonably believe to be a victim of abuse, neglect or domestic violence to a governmental authority (including a social service or protective services agency) authorized by law to receive reports of abuse, neglect or domestic violence in any of the following three (3) circumstances:
   a. Where the disclosure is required by law and the disclosure complies with and is limited to the requirements of the law;
   b. If the individual agrees to the disclosure; or
   c. To the extent that the disclosure is expressly authorized by statute or regulation, and either of the following are applicable:
      i. We believe the disclosure is necessary to prevent serious harm to the individual or other potential victims; or
      ii. 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 personal information 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.

   When we make a permitted disclosure about a victim of abuse, neglect, or domestic violence, we will promptly inform the individual who is the victim that a disclosure has been, or will be, made except if:

When we make a permitted disclosure about a victim of abuse, neglect, or domestic violence, we will promptly inform the individual who is the victim that a disclosure has been, or will be, made except if:

a. We, in the exercise of professional judgment, believe informing the individual would place the individual at risk of serious harm; or

b. We would be informing a personal representative (such as a family member or friend), and we reasonably believe 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 we determine in the exercise of professional judgment.

8. To a law enforcement official for a law enforcement purpose (if consistent with applicable law and standards of ethical conduct) under any of these circumstances:

   a. In response to a lawful court order, court-ordered warrant, subpoena or summons issued by a judicial officer, or a grand jury subpoena;

   b. If the law enforcement official makes a written request for personal information that:

      i. Is signed by a supervisory official of the law enforcement agency seeking the personal information;

      ii. States that the information is relevant and material to a legitimate law enforcement investigation;

      iii. Identifies the personal information sought;

      iv. Is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and

      v. States that de-identified information could not be used to accomplish the purpose of the disclosure.

   c. If we believe in good faith that the personal information constitutes evidence of criminal conduct that occurred on our premises

   d. In response to an oral request for the purpose of identifying or locating a suspect, fugitive, material witness or missing person and the personal information disclosed consists only of name, address, date of birth, place of birth, Social Security Number, and distinguishing physical characteristics; or

   e. If the official is an authorized federal official seeking personal information for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879 (threats against the President and others) and the information requested is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought.

9. To comply with government reporting obligations for HMIS and for oversight of compliance with the HMIS requirements.

10. To a law enforcement official for a law enforcement purpose (if consistent with applicable law and standards of ethical conduct) under any of these circumstances:

   a. Where the disclosure is required by law and the disclosure complies with and is limited to the requirements of the law;

   b. In response to a lawful court order, court-ordered warrant, subpoena or summons issued by a judicial officer, or a grand jury subpoena;

   c. If the law enforcement official makes a written request for personal information that:

      i. Is signed by a supervisory official of the law enforcement agency seeking the personal information;

      ii. States that the information is relevant and material to a legitimate law enforcement investigation;

      iii. Identifies the personal information sought;

      iv. Is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and

      v. States that de-identified information could not be used to accomplish the purpose of the disclosure.

   d. If we believe in good faith that the personal information constitutes evidence of criminal conduct that occurred on our premises

   e. In response to an oral request for the purpose of identifying or locating a suspect, fugitive, material witness or missing person and the personal information disclosed consists only of name, address, date of birth, place of birth, Social Security Number, and distinguishing physical characteristics; or

   f. If the official is an authorized federal official seeking personal information for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879 (threats against the President and others) and the information requested is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought.

11. For academic research purposes:

   a. Conducted by an individual or institution that has a formal relationship with the covered homeless organization (CHO) if the research is conducted either:

      i. By an individual employed by or affiliated with the organization for use in a research project conducted under a written research agreement approved in writing by a designated CHO program administrator (other than the individual conducting the research), or

ii. By and institution for use in a research project conducted under a written research agreement approved by a designated CHO administrator; and

b. Any written research agreement:

i. Must establish rules and limitations for the processing and security of PPI in the course of the research;

ii. Must provide for the return or proper disposal of all PPI at the conclusion of the research;

iii. Must restrict additional use or disclosure of PPI, except where required by law;

iv. Must require that the recipient of data formally agree to comply with all terms and conditions of the agreement; and

v. Is not a substitute for approval (if appropriate) of a research project by an Institutional Review Board, Privacy Board, or other applicable human subjects protection institution.

12. To comply with government reporting obligations for HMIS and for oversight of compliance with the HMIS requirements.

IV. HOW TO INSPECT AND CORRECT PERSONAL INFORMATION

A. You may inspect and have a copy of your personal information that we maintain. We will offer to explain any information that you may not understand.

B. We will consider a request from you for correction of inaccurate or incomplete personal information that we maintain about you. If we agree that the information is inaccurate or incomplete, we may delete it or we may choose to mark it as inaccurate or incomplete and to supplement it with additional information.

C. To inspect, receive a copy of, or ask for correction of your information:

1. Please complete a request to review or receive a copy of your Personal Information: This is a Personal Information Review (PIR) form. A copy of information that we maintain about you will be available to you by the end of our next business day.

2. The PIR can then be examined for accuracy and completeness. If accuracy and completeness need to be addressed, please note those concerns on a copy of the PIR and request those changes. Staff will review and make an appointment to discuss these requested changes within 7 working days of the receipt of the requested changes on the PIR copy.

D. We may deny your request for inspection or copying of personal information if:

1. The information was compiled in reasonable anticipation of litigation or comparable proceedings;

2. The information is about another individual (other than healthcare or homeless providers);

3. The information was obtained under a promise or confidentiality (other than a

promise from a health care provider or homeless provider) and if the disclosure would reveal the source of the information; or

4. Disclosure of the information would be reasonably likely to endanger the life or physical safety of any individual.

E. If we deny a request for access or correction, we will explain the reason for the denial. We will also include, as part of the personal information that we maintain, documentation of the request and the reason for the denial

F. We may reject repeated or harassing requests for access to or correction of personal information.

V. DATA QUALITY & RETENTION

A. We collect only personal information that is relevant to the purposes for which we plan to use it. To the extent necessary for those purposes, we seek to maintain only personal information that is accurate, complete, and timely.

B. We will dispose of personal information not in current use seven (7) years after the information was created or last changed. As an alternative to disposal, we may choose to remove identifiers from the information.

C. We may keep information for a longer period if required to do so by an applicable statute, regulation, contract, or other requirement.

VI. COMPLAINTS AND ACCOUNTABILITY

A. We accept and consider questions or complaints about our privacy and security policies and practices.

1. Any questions or complaints regarding our privacy and security policies and practices should be addressed to the following:

    HMIS Lead Agency,
    Mendocino County HHSA
    747 S. State Street, Ukiah, CA 95482
    (707) 463-7900

B. All members of our staff (including employees, volunteers, affiliates, contractors and associates) are required to comply with this privacy Policy. Each staff member must receive a copy of this privacy policy.

Appendix D: HMIS Informed Consent & ROI Authorization Form

Mendocino County Homeless Services Continuum of Care
Homeless Management Information System (HMIS)
Informed Consent & Release of Information Authorization Form

IMPORTANT: Do not enter personally identifying information into HMIS for clients who are: 1) in Domestic Violence Agencies or; 2) currently fleeing or in danger from a domestic violence, dating violence or sexual assault or stalking situation. If this applies to you, STOP – DO NOT sign this form.

This Agency participates in the Mendocino County Homeless Services Continuum of Care, a collaborative group of partner agencies working together to provide services to individuals and families in Mendocino County who are homeless or at risk of becoming homeless. To provide the most effective services in moving people from homelessness to permanent housing, we need an accurate count of all people experiencing homelessness in Mendocino County.

- Information collected includes: name, social security number, date of birth, race, ethnicity, gender, veteran status, address history, program entry and exit dates, length of time homeless, housing status, income and sources, non-cash benefits, physical or developmental disability, chronic health condition, HIV/AIDS, behavioral health, substance abuse, health insurance, domestic violence, services provided, and residential move-in date.
- The data provided will be combined with data from the Department of Health and Human Services for the purposes of: (a) providing individual case management including participation in Case Conferencing for individuals participant needs; (b) producing reports to analyze utilization of services; (c) tracking individual outcomes; (d) providing accountability for individuals and entities that provide funds for use in Mendocino County; (e) identifying homeless service needs and plan for the provision of new services; (f) allocating resources among agencies engaged in the provision of services in and around Mendocino County; and (g) for all other purposes deemed appropriate by ____.
- Your name and other identifying information will not be included in any reports or publications. Only a limited number of staff members employed by agencies participating in the Mendocino County Homeless Services Continuum of Care who have signed confidentiality agreements will have access to this information. Your information will not be used to determine eligibility for programs. Current HMIS agencies are: Adventist Health Ukiah Valley, Community Development Commission of Mendocino County, City of Fort Bragg, Ford Street Project, Manzanita Services, MCAVHN Care and Prevention Network, Mendocino Coast Hospitality Center, Mendocino Community Health Clinic, Mendocino County HHSA – Social Services, Mendocino County Youth Project, Redwood Community Services, Redwood Quality Management Company, Rural Community Housing Development Corporation, San Francisco VA Health Care System, and Willits Community Services.
- Your decision to participate in HMIS will not affect the quality or quantity of services you are eligible to receive from this Agency and will not be used to deny outreach, assistance, shelter, or housing. However, if you do choose to participate, services in the region may improve if we have accurate information about homeless individuals and the services they need. Furthermore, some funders MAY require that you consent to your information being entered in HMIS for you to receive services from that funding source.
- We will guard this information with strict policies to protect your privacy. Our computer system is highly secure and uses up-to-date protection features, such as data encryption, passwords, and identity checks required for each system user. If you ever suspect the data in HMIS has been misused, immediately contact the HMIS System Administrator at: 747 S. State St, Ukiah, CA 95482; 707-463-7900; fax 707-463-7979.

Mendocino County Homeless Services Continuum of Care
Homeless Management Information System (HMIS)
Informed Consent & Release of Information Authorization Form

Initials

______ I understand the above statements and consent to the inclusion of personal information in HMIS about me and any dependents listed below, and authorize information collected to be shared with partner agencies. I understand that my personal information will not be made public and will only be used with strict confidentiality. I also understand that I may withdraw my consent at any time by supplying a written request form to this Agency.
Federal laws and regulations do not protect any information about suspected child or elder abuse or neglect from being reported under state law to appropriate state or local authorities. (See 42 USC 290dd-2 for federal law and 42CFR Part 2 for federal regulations.)

______ I understand and acknowledge that the data pertaining to the services provided to me by the Agency and the records maintained by the Agency may include medical/health and other information, the privacy of which may be protected by federal and/or California law, and expressly consent to the release of such information as well as the information expressed in the sections above regarding crimes and child abuse/neglect.

______ I understand this authorization will remain in effect for seven (7) years from the date of my signature unless revoked in writing to this Agency. If I revoke my authorization, all information about me already in the database will remain but will become invisible to partner agencies.

Specify data (if any) you wish to restrict from entry into the HMIS:

____

____

Dependent children under age 18 in household, if any (please print first and last names):

______________________________ ______________________________

______________________________ ______________________________

______________________________ ______________________________

______________________________ ______________________________

Participant Print Name Staff Printed Name

X_____________________________ X_____________________________

Participant Signature (Parent/Guardian) Staff Signature

______________________________ ______________________________

Date Date

(Each adult age 18 years and older must sign a separate release form)