



Homeless Management Information System (HMIS) Policies and Procedures

Ending Homelessness

Homelessness is a humanitarian crisis that impacts all our communities in Sonoma County. Ending homelessness requires a countywide, shared responsibility in planning and developing solutions. The Sonoma County Homeless Coalition is the region-wide body responsible for setting the vision and strategic planning towards ending homelessness in Sonoma County. The goal of the Sonoma County Homeless Coalition is to achieve “functional zero” homelessness in Sonoma County through a Housing First strategy. Through the Sonoma County Homeless Coalition, persons experiencing homelessness will be connected to permanent housing as quickly as possible using a Coordinated Entry System, Rapid Re-Housing, and Permanent Supportive Housing as key strategies to end individual housing crises. As both a funding agency and convener of planning efforts, the Sonoma County Department of Health Services acts as the Lead Agency for the Sonoma County Homeless Coalition. In partnership with service agencies, advocates, and the community, our goal is to make homelessness increasingly rare and brief.

Table of Contents

Table of Contents.....	3
Introduction.....	6
What is HMIS and Its Purpose.....	7
Governing Principles	8
Key Support Roles & Responsibilities	9
Homeless Coalition Board	9
HMIS Management Team (Sonoma County Department of Health Services- lead agency).....	10
HMIS Coordinator	11
Partner Agency Technical Administrator	12
Partner Agency Security Officer.....	14
End User.....	15
HMIS Operating Procedures.....	15
Agency Implementation Policies.....	16
HMIS Project Participation Policy.....	16
For Agencies participating in Coordinated Entry.....	16
Minimum Participation Standards	17
Data Collection	18
HMIS Partnership Violations and Termination – Data Transfer Policies.....	19
Sequence of Procedures.....	19
Reinstatement.....	23
HMIS Security Plan	24
Hardware, Connectivity, and Security	24
Workstation Access Restrictions	24
Workforce Access Restrictions.....	25
Establishing End-user Access	25
End User’s Access Levels	26
Data Access & Password Policies	27
Rescind User Access.....	28

Special Considerations	28
Virus Protection	28
Firewall.....	29
Disaster Recovery	29
Security Audits.....	30
Ongoing Monitoring	30
Enforcement Policies.....	30
HMIS Privacy Plan.....	31
Client Notification & Client Consent.....	31
Specific Client Notification for Victims of Domestic Violence	34
Privacy Compliance & Grievance Policy	34
Unauthorized Release of information	35
Corrective Action Plan Policy and Procedure	35
Sonoma County HMIS Corrective Action Plan.....	39
HMIS Data Quality Plan.....	40
What is Data Quality?.....	40
Components of a Data Quality Plan	40
Identifying and Correcting Errors in ETO HMIS	42
HMIS Bed Coverage.....	44
Data Quality Training/ Performance Monitoring- HMIS	45
Deduplication of Data	45
Technical Support.....	46
User Training	47
HMIS Security and Ethics Training.....	47
HMIS New User Orientation	47
Agency/User Forms-.....	47
Report Generation.....	48
HMIS Provider Database.....	48
Provider Agency’s Reporting Responsibilities	48
Community Data Requests (Non-HMIS Agencies/Organizations)	50

Local Changes to HMIS Policies & Procedures and other Documents.....	50
Other Obligations and Agreements.....	51
Forms Control.....	51
Development and Maintenance of Required HMIS Policies and Standards.....	51
Glossary of Terms.....	52

Approved and adopted the 24th day of February, 2021. These policies and procedures replace the HMIS Procedures Manual approved on August 30, 2018. I, the undersigned, hereby certify that the foregoing Governance Charter was duly adopted by the Sonoma County Homeless Coalition Board:

Following Roll Call Vote: Ayes: 14
 Nos: 0
 Absent: 1

Benjamin Leroi, Homeless Coalition Board Chair

Introduction

This document provides the framework for the ongoing operations of the Homeless Management Information System (HMIS) for the Sonoma County Homeless Coalition.

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

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

All HMIS End Users are required to read and comply with the HMIS Data and Technical Standards. Failure to comply with the HUD standards carries the same consequences as failure to comply with these Policies and Procedures. In any instance where these Policies and Procedures and Security Plan are not consistent with the HUD HMIS Standards, the HUD Standards take precedence. Should any inconsistencies be identified, please immediately notify the HMIS Lead Agency.

For agencies or programs where HIPAA applies, HIPAA requirements take precedence over both the HUD HMIS Data Requirements (as specified in those requirements) and these Policies and Procedures. Agencies and programs are responsible for ensuring HIPAA compliance.

The Project Overview provides the main objectives, direction and benefits of HMIS. Governing Principles establish the values that are the basis for all policy statements and subsequent decisions. Operating Procedures include the HMIS Privacy Plan and Security Plan which provides specific policies and steps necessary to control the operational environment and enforce compliance in project participation, workstation security, user authorization and passwords, training of collection and entry of client data, release and disclosure of client data, training, compliance, and technical support. HMIS Data Quality Plan provides specific rules on specific data points that need to be added to the system per funding source including the timeframe when data needs to be entered. The Other Obligations and Agreements section discusses additional considerations of this project, and the Forms Control section provides information on obtaining and updating forms, filing and record keeping.

What is HMIS and Its Purpose

The long-term vision of HMIS is to enhance Partner Agencies' collaboration, service delivery and data collection capabilities. Accurate information will put the collaborative in a better position to request funding from various sources and help better plan for future needs. The purpose of the Sonoma County HMIS is to be an integrated network of homeless and other services providers that use a central database to collect, track and report uniform information on client needs and services. This system will not only meet federal requirements, but also enhance service planning and delivery. The fundamental goal of the Sonoma County HMIS is to document the demographics of homelessness in Sonoma County according to the HUD HMIS standards. It is then the goal of the project to identify patterns in the utilization of assistance, and document the effectiveness of the services for the client. This will be accomplished through analysis of data that is gathered from actual experiences of homeless persons, the service providers who assist them in shelters, and other homeless assistance programs throughout the counties. Data that is gathered via intake interviews and program participation will be used to complete HUD annual progress reports. This data may also be analyzed to provide unduplicated counts and anonymous data to policy makers, service providers, advocates, and consumer representatives.

Sonoma has chosen Efforts to Outcomes by Social Solutions as its web-enabled HMIS application residing on a vendor hosted central server to facilitate data collection by homeless service organizations across the county. Access to the central server is limited to agencies formally participating in the project including only authorized staff members that have met the necessary training and security requirements.

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

Service coordination can be improved when information is shared, with written client consent, among case management staff within one agency or with staff in other agencies who are serving the same clients. Better service coordination leads to a shorter time to housing.

Potential benefits for agencies and program managers:

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

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

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

Governing Principles

All End Users are expected to read, understand, and adhere to these *Governance Policies and Procedures*. Described below are the overall governing principles upon which all decisions pertaining to the Sonoma County's HMIS are based:

Clients can control what is being entered into HMIS. Each individual client can grant informed consent, limited data sharing, be entered as anonymous or revoke consent to their information at any time.

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

End Users are to strive for the highest possible degree of data quality. As poor data quality can lead to reduction in funding for service.

Confidentiality

The rights and privileges of clients are crucial to the success of HMIS. These policies will ensure clients' privacy without impacting the delivery of services. Policies regarding client data will be founded on the premise that a client owns his/her own personal information and will provide the necessary safeguards to protect client, agency, and policy level interests. Collection, access and disclosure of client data through HMIS will only be permitted by the procedures set forth in this document.

Data Integrity

Client data is the most valuable and sensitive asset of the Sonoma County's HMIS. These policies will ensure integrity and protect this asset from accidental or intentional unauthorized modification, destruction or disclosure.

System Availability

Sonoma County HMIS is hosted and maintained by Social Solutions. It is Social Solutions responsibility to maintain System Availability for homeless service Agencies in Sonoma County. The System is available and accessible through a modern internet browser.

Compliance

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

Key Support Roles & Responsibilities

Homeless Coalition Board

Sonoma County's primary decision-making group regarding homelessness services, housing and funding is the Sonoma County Homeless Coalition Board. This fifteen-member public-private decision-making body will align funding and policy to address homelessness throughout the County and serves as the county's Continuum of Care Board to address HUD requirements. The board must be a subset of the CoC membership that is established in accordance with the CoC regulations governing board composition (*Please refer to the Sonoma County Continuum of Care Governance Charter for details*).

Responsibilities

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

HMIS Management Team (Sonoma County Department of Health Services-lead agency)

In an effective system of care, Lead Agency professional staff play a key role, serving as a bridge between the Homeless Coalition Board and the CoC Board developed Committee's. The Lead Agency is responsible for providing support, data, and accountability for both groups as well as filling the role of Collaborative Applicant for HUD-mandated Continuum of Care responsibilities. The Sonoma County Department of Health Services (the Department) serves as the Lead Agency. The Sonoma County Homeless Coalition Board may revisit the Lead Agency designation at its discretion.

Responsibilities

- a. Serve as the Lead Agency for the Sonoma County Continuum of Care.
- b. Develop, review, and revise all HMIS plans, forms, standards and governance documents.
- c. Prepare Sonoma County System Performance Measures, AHAR/Longitudinal System Analysis, and other data submissions, in alignment with HUD requirements.
- d. Develop and implement a process for accepting additions to the CoC Board's Committee's.
- e. Staff the CoC Board and Committee's.

- f. Ensure that all data is reported accurately and with integrity so that the CoC Board has confidence in the credibility of all reported data presented to its members.
- g. Protect all Personally Identifiable Information (PII) in accordance with HUD guidelines.
- h. Liaison with Housing and Urban Development(HUD)
- i. Serves as Liaison and Executes contract with HMIS software vendor
- j. Liaison with Partner Agencies to ensure they meet HMIS requirements
- k. Executing and maintaining copies of signed Participation Agreements
- l. Monitoring and providing regular reports to the CoC Board.
- m. Configuring HMIS software to meet needs of Partner Agencies and CoC
- n. Oversee HMIS licensing- procuring, issuing, removal
- o. Provide End User technical support or operation issues
- p. Oversees all training of Provider Agency Leads and End-users.
- q. Oversees system-wide reporting including ETO results and operating reporting tools such as Excel, Crystal Reports and others.
- r. Develops documentation of created reports.

HMIS Coordinator

The HMIS Coordinator is an employee of the HMIS Lead agency and is the primary point of contact for all service providers for matters relating to HMIS.

Responsibilities

- a. Database
 - Oversees HMIS project performance.
 - Responds to system needs.
 - Oversees all training of Provider Agency Leads and End-users.
- b. Support
 - Oversees Help-Desk function.
 - Oversees HMIS technical support services.
 - Supervises internal and external security protocols.
 - Addresses HMIS technical operational issues.
- c. Data integrity
 - Monitors operation of the HMIS database.
 - Monitors and evaluates the quality, timeliness, and accuracy of data input, data management, and data reports.
 - Assists HMIS Users.
 - Identifies and addresses potential operational issues with individual Provider Agencies, the HMIS Users, the CoC Board, and relevant parties
- d. Reports

- Oversees system-wide reporting.
- Writes detail report specifications based on requests from the User Group and Project Team.
- Generates reports using ETO Results
- Understands and operates reporting tools such as Excel, Crystal Reports and others.
- Develops documentation of created reports.

Partner Agency Technical Administrator

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

Responsibilities

- Overseeing agency compliance with the Participation Agreement and all applicable plans, forms, standards and governance documents.
- Detecting and responding to violations of any applicable HMIS plans, forms, standards and governance documents.
- Serving as the primary contact for all communication regarding the HMIS at this agency and forwarding information to all agency End Users as appropriate.
- Ensuring thorough and accurate data collection by agency End Users as specified by HMIS forms and standards.
- Provides technical support assistance to agency's End-users.
- Monitors End-user compliance in regard to confidentiality, and data integrity:
 - Is responsible for insuring appropriate use of the database by Provider Agency's designated staff.
 - Allows HMIS database access only to qualified End-users based upon job description and need to access.
 - Reviews HMIS Policies and Procedures with all End-users, both new and old.
- Develops and maintains **internal** policies and procedures to ensure:
 - New and continued staff training.
 - Timely and accurate input of HMIS data.
 - Personnel procedures addressing violations of the HMIS Code of Ethics.
 - Protocols for data access and reporting.
- Maintaining agency and program descriptor data in HMIS,

- i. Ensuring all users adhere to trainings provided by Sonoma County, and ETO. Providing licenses for HMIS System only after the authorized End-users completes all necessary training and signs documents outlined in End-user Training Guide.
- j. Performing authorized imports of client data.
- k. Updates Provider Agency and End-users on decisions made during Data Group meetings.

- **Quarterly Provider Meetings**

- i. Purposes:

- 1. Opportunity for Benchmarking between participants
 - 2. Review core processes and related measures
 - 3. Identify issues and share solutions
 - 4. Identify those issues where additional help is needed
 - 5. Incorporate process and outcome measures (For example Sonoma County CoC HMIS Project requires coverage rate types of reports generated at the Provider Agency level)
 - 6. Support transparency
 - 7. Share successes
 - 8. Review aggregated data
 - 9. Formalize communication between Provider Agency and System Administrators
 - 10. Provides routine End-user satisfaction input

- ii. Types and Frequencies

- 1. Agency Administrator / User Group Meetings – Quarterly
 - 2. Data Committee – monthly
 - 3. Specialty Provider Agency Meetings (as needed):
 - a. Domestic Violence
 - b. Runaway Youth
 - c. Housing Specialists
 - d. Mental Health
 - e. Homeless Education Providers

- iii. Meeting Requirements

- 1. Minimum attendance levels (= all those with End-user licenses + leadership)
 - 2. Structured Meeting Agenda reviewing core processes:
 - a. Coverage – Are all the clients being entered? What % of the homeless are in the System?
 - b. Client Refusals
 - c. Data Quality – null data fields, # of data corrections
 - d. Interview issues
 - e. Definition questions

- f. Training needs
 - g. Privacy and Security issues
 - h. Reports: Review Provider
 - i. Agency aggregated data
 - j. Structured Minutes with copy sent to System Administrator to monitor End-user meeting compliance with the Sonoma County CoC HMIS Project contract
- iv. Additional Processes related to System Administrator and Sonoma County CoC HMIS Project Meetings
 - 1. System Access / Licenses
 - 2. System Performance
 - 3. Routine Support
 - 4. Contract Compliance

Partner Agency Security Officer

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

Responsibilities

- a. Conduct a thorough quarterly review of internal compliance with all applicable HMIS plans, standards and governance documents.
- b. Completing the Compliance Certification Checklist and forwarding the Checklist to HMIS Coordinator at least once per year.
- c. Continually monitoring and maintaining security of all staff workstations used for HMIS data entry.
- d. Safeguarding client privacy by ensuring End User and agency compliance with confidentiality and security policies.
- e. Investigating potential breaches of HMIS system security and/or client confidentiality and notifying Sonoma County of substantiated incidents.
- f. Developing and implementing procedures for managing new, retired, and compromised local system account credentials.
- g. Developing and implementing procedures that will prevent unauthorized users from connecting to private agency networks.

- h. Ensure proper agency workstation configuration and for protecting their access by all agency users to the wider system.
- i. Assumes responsibility for integrity and protection of client information entered into the HMIS database.
- j. Update virus protection software on agency computers that accesses the HMIS database on a scheduled, regular basis.
- k. Ensuring the agency provides and maintains adequate internet connectivity.
- l. Provides manual data entry processes in the event of a HMIS disaster.
- m. Monitors End-user compliance in regard to security.
- n. Is responsible for insuring appropriate use of the database by Provider Agency's designated staff.

End User

Each agency will have 1 or more end users that will be responsible for timely data entry into the HMIS. Only those parties authorized for the following reasons may be provided access to the HMIS:

- a. Data entry
- b. Editing Client records
- c. Viewing Client records
- d. Report writing
- e. Administration
- f. Other essential activities associated with HMIS Provider Agency business use

Responsibilities

- a. Entry client data into HMIS
- b. Meet data entry timeliness
- c. Adhere to HMIS and Provider Agency Policy and Procedures
- d. Protect HMIS and Provider Agency data and information
- e. Prevent unauthorized disclosure of data
- f. Report Security Violations to Agency Administrator
- g. Remain accountable for all actions undertaken with his/her End-user name and password

HMIS Operating Procedures

Agency Implementation Policies

- a. Sign HMIS Agency Participation Agreement.
- b. Set up End-user identification and grant access to the database based upon the End-user's job description.

HMIS Project Participation Policy

Agencies participating in the Sonoma County HMIS Project shall commit to abide by the governing principles of the Sonoma County HMIS Project and adhere to the terms and conditions of this partnership as detailed in the Participation Agreement. Agencies receiving Continuum of Care Program or Emergency Solutions Grant funding are required to participate in HMIS.

Responsibilities

- a. The Partner Agency, (referred to by HUD as Contributing Homeless Organizations or CHOs) shall confirm its participation in HMIS and commitment to these Policies and Procedures by submitting a Participation Agreement signed by the Partner Agency's Executive Director to the HMIS Lead Agency. The HMIS Lead Agency will return a copy of the countersigned Participation Agreement to the Partner Agency's Technical Administrator and/or Executive Director.
- b. At the time the Partner Agency begins participating in HMIS, it must designate at least one Technical Administrator who must obtain an HMIS license. If the Technical Administrator is not the same person as the Executive Director, then the Technical Administrator must also sign the Participation Agreement. In either case, the Technical Administrator must be listed in writing on the Participation Agreement. If a new Technical Administrator later takes over this responsibility, the change must be recorded in writing and communicated to the HMIS Lead.
- c. The HMIS Lead Agency will maintain a file of all signed Participation Agreements.
- d. Each Partner Agency shall re-confirm the agency's participation in HMIS and commitment.
- e. The HMIS Lead Agency will maintain and publicly publish a list of all current Partner Agencies on the HMIS web portal.

For Agencies participating in Coordinated Entry

The HMIS is key to centralizing information to measure outcomes and determine client needs through Coordinated Entry. Not all stakeholders have direct access to HMIS. Throughout the CoC, service provider agencies that directly interact with people facing homelessness actively use and contribute to the HMIS. All HMIS Lead personnel (including employees, volunteers, affiliates, contractors and associates), and all participating agencies and their personnel, are

required to comply with the HMIS User Policy, Agency Participation Agreement, and Code of Ethics Agreement. All personnel in the CES participating agencies with access to HMIS must receive and acknowledge receipt of a copy of the Participation Agreement and receive training on this Privacy Policy before being given access to HMIS.

To comply with federal, state, local, and funder requirements, information about the homeless persons, their dependents, and the services that are provided to them, is required to be collected in the HMIS. When assistance is requested, it is assumed that the client is consenting (“inferred consent”) to the use of the HMIS to store this information. The participants have the right to explicitly refuse the collection of this information, and participating agencies are not permitted to deny services for this reason. However, such refusal may severely impact the ability of any participating agency throughout the CES to qualify the client for certain types of assistance or to meet their needs.

Data collection should not be confused with data sharing (“disclosure”). Participating agencies are required to provide the client with an opportunity to consent to certain disclosure of their information with CE and cooperating agencies, either in writing or electronically. If the client consents to the disclosure of their information, they enhance the ability of CE to assess their specific needs and to coordinate delivery of services for them.

To protect the privacy and the security of client information, the HMIS is governed by data access control policies and procedures. Every user’s access to the system is defined by their user type and role. Their access privileges are regularly reviewed, and access is terminated when users no longer require that access. Controls and guidelines around password protection and resets, temporary suspensions of User Access and electronic data controls are in place and are outlined in detail in the HMIS User Agreement. Services will not be denied if the participant refuses to allow their data to be shared, unless Federal statute requires collection, use, storage and reporting of a participant’s personally identifiable information as a condition of program participation.

HMIS users will be informed and understand the privacy rules associated with collection, management, and reporting of client data.

Minimum Participation Standards

Partner agencies must collect the required Universal and Program Specific data elements required for their funding source as required in the HUD HMIS Data standards manual, and the HMIS program manual for that funding source if applicable. Non funded agencies must collect data elements required for their project type to be considered participating.

As referenced below:

Universal Data Elements:

Name
Social Security
Date of Birth
Race
Ethnicity
Gender
Veteran Status
Disabling Condition
Project Start Date
Project Exit Date
Destination
Relationship to Head of Household
Client Location
Housing Move –in Date
Prior Living Situation (3.917A or 3.917B)

Program Specific Data Elements:

Income and Sources
Non-Cash Benefits
Health Insurance
Physical Disability
Developmental Disability
HIV/AIDS
Mental Health Problem
Substance Abuse
Domestic Violence
Current Living Situation
Data of Engagement
Bed-night Date
Coordinated Entry Assessment
Coordinated Entry Event

All data must be entered in a timely manner and be checked for accuracy.

Data Collection

Provider Agency will:

- a. Assume responsibility for End-user's data entry and accuracy.
 - View, obtain, disclose, or use the database information only for business purposes related to serving the Provider Agency's clients.
- b. Monitor End-user data entered into the HMIS database, in accordance with Provider Agency's policies and the HMIS minimum data standards.
- c. Not delete a client profile created by another Provider Agency.
- d. Correct inaccurate information and missing required data elements.
- e. **Not** misrepresent the number of clients served or the types of services/beds provided.
 - Only view, obtain, disclose, or use the database information for business purposes related to serving the Provider Agency's clients.
 - Enter data into the HMIS database in accordance with the Provider Agency's policies and the Sonoma County CoC HMIS minimum data standards.
 - Not enter any fictitious or misleading client data.
 - Not over-ride or delete information entered by another End-user.
 - Edit and/or delete only screens entered by the individual End-user.
 - Save data entered at regular intervals. (If the system remains inactive for longer than fifteen minutes, it will automatically log the End-user off the database and not save entered data.)

- f. Client data will be entered into the HMIS in a timely manner.
- g. Client identification should be completed during the intake process or as soon as possible following intake and within 5 calendar days.
- h. Service records should be entered on the day services began or as soon as possible within 5 calendar days.
- i. Required assessments should be entered as soon as possible following the intake process and within 5 calendar days.
- j. Do not enter discriminatory comments made by or about an employee, volunteer, client, or any person based on race, color, religion, national origin, ancestry, handicap, age, sex, and sexual orientation unless direct quotes are deemed essential for assessment, service, and treatment purposes.
- k. Not enter offensive language and profanity into the HMIS database unless direct client quotes are deemed essential for assessment, service, and treatment purposes.
- l. Hardcopy and electronic files will continue to be maintained according to individual program requirements in accordance with the HUD Data Standards.

HMIS Partnership Violations and Termination – Data Transfer Policies

Sequence of Procedures

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

- In emergency situations i.e. security breach and/or imminent danger to the database, the HMIS Coordinator immediately contacts and reports to Sonoma County Department of Health Services' (SCDHS) Ending Homelessness Manager, who has final authority for the impending action.
- In all other cases, the HMIS Coordinator implements a course of action outlined in the following steps:

- Step 1: Consultation with the Provider Agency
- Step 2: Written warning
- Step 3: Sanctions
- Step 4: Probation
- Step 5: Suspension
- Step 6: Termination

Step 1: Consultation with the Provider Agency. The HMIS Coordinator:

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

Step 2: Written Warning

- a. If any corrective measures do not happen, or if inappropriate practices continue over multiple months, then the HMIS Coordinator, under the guidance of the Data Committee, and SCDHS Administrators, implements a written warning procedure.
- b. The HMIS Coordinator or an appropriate HMIS staff member (under the HMIS Coordinator instruction) sends a written notice, via certified mail, to the Provider Agency Administrator which includes:
 - An explanation of violations and itemizes specific requirements for improvement as defined through a Corrective Action Plan. (See Corrective Action Plan Policy)
 - A time frame for implementation and completion of the corrective measure(s).
 - A copy of the written summary documenting the HMIS Coordinators, User Group and SCDHS Ending Homelessness Managers review of the Provider Agency's profile.
 - A training or technical assistance plan, if deemed necessary.
 - Further HMIS actions if the inappropriate practice(s) continue.
- c. The technical support staff archives a copy of the written warning in the Provider Agency's file, the Provider Agency receives the original written notice.

Step 3: Sanctions

- a. If the Provider Agency fails to provide satisfactory responses to the written warning within the allotted time period, as defined in the Corrective Action Plan, then the HMIS Coordinator presents the updated Provider Agency file to the Data Committee and SCDHS Ending Homelessness Manager.

- b. The Data Committee and SCDHS Ending Homelessness Manager review all previous correspondences and/or Provider Agency corrective action responses and determine sanctions based on the evidence.
- c. The HMIS Coordinator notifies via certified mail the Provider Agency of impending sanctions, the effective date, a copy of the original written notice, a copy of the HMIS Grievance Policy and this policy.
- d. The technical support staff archives a copy of the sanctions notification in the Provider Agency's file, the Provider Agency receives the original written notice.

Step 4: Probation

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

The notification:

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

Step 5: Suspension

- a. If the Probationary Provider Agency's inappropriate practice(s) continues or reoccurs, and there is no resolution with the HMIS Coordinator and HMIS staff satisfactory to the Data Committee and SCDHS Ending Homelessness Manager, then the HMIS Coordinator begins the suspension process.

- The HMIS Coordinator:
 1. Notifies via certified mail the Provider Agency of impending suspension and the effective date.
 2. Assigns appropriate HMIS staff to facilitate data identification and data transfer to another database.
 3. Immediately inactivates all Provider Agency End-user database access.
 4. Only reactivates End-user access after receiving written permission via email or fax from the Data Committee and/or SCDHS Ending Homelessness Manager.
- The notification:
 1. Identifies assigned HMIS staff, who will work collectively with the Provider Agency Administrator and Executive Director, to identify and transfer database elements needed for the Provider Agency to continue conducting business.
 2. Includes an updated copy of the Data Committee and SCDHS Ending Homelessness Manager's review and decision to suspend Provider Agency's HMIS access.
 3. Explains the change in provider status to Suspended Provider Agency and the suspension of all End-user database access.
 4. Explains the requirement of a mandatory meeting to address the resolution of inappropriate practices. The HMIS Coordinator coordinates the meeting time and place with all participants, which include the Agency Administrator and/or the Executive Director, Data Committee representatives and SCDHS Ending Homelessness Manager.
 5. Explains the possibility of the Provider Agency losing HUD funding.

b. The technical support staff archives a copy of the suspension notification in the Provider Agency's file; the Provider Agency receives the original written notice.

Step 6: Termination

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

- i. Must submit a request for their data within 60 days of termination.
 - ii. Assumes responsibility for cost of data transfer to another database.
 - iii. Pays the HMIS accountant prior to data delivery.
- The SCDHS Ending Homelessness Manager, in conjunction with Social Solutions Group, provides a detailed cost analysis and timeline of data transfer.
- c. The Social Solutions Group will provide the data file in ASCII delimited format only.

Reinstatement

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

Reinstatement Process:

Terminated Provider Agency:

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

HMIS Coordinator:

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

Ending Homelessness Manager:

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

HMIS Coordinator:

1. Provides reinstatement date to the Provider Agency.
2. Re-activates Provider Agency's Probationary Status.

3. Instructs HMIS staff to begin coordinating time-line dates and corrective changes into the monitoring procedure.

HMIS Staff:

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

HMIS Security Plan

Hardware, Connectivity, and Security

Malicious codes, delivered through various means, are designed to delete, scramble End-user files/ programs and/or disable specific computer functions. At times a malicious code slows down a computer--- a mere inconvenience; other times, a malicious code causes an entire system to shut down.

Since the computer industry progresses rapidly, each Provider Agency must keep current on protective procedures by consulting with computer system experts periodically for the latest in malicious code preventative measures.

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

Workstation Access Restrictions

Agency Workstation Minimum requirements:

Computer workstations must be connected to the internet to access HMIS.

Recommended Internet connection: Wired, or Secure Wireless connection

Recommended Browsers: is compatible with Chrome, Firefox, Edge, and iOS Safari. And must have an antivirus with the latest virus definitions.

Access to the HMIS database should only be from pre-determined work terminals. HMIS should only be accessed through secure workstations and prohibited on public workstations (libraries, cafes, etc.).

End-user Requirements:

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

Workforce Access Restrictions

Each participating agency must conduct a criminal background check on each of its Partner Agency HMIS Administrators and Security officers at its own expense. The Partner Agency's Executive Director will evaluate the results of the criminal background checks for any concerns. To protect the security and integrity of the HMIS system and safeguard the personal information contained therein, the Partner Agency's Executive Director must consider the results of the background check on a case-by-case basis.

- a. An individual whose background raises concerns about whether s/he may sufficiently be relied upon to help the HMIS Lead Agency achieve this goal may not initially be given administrative-level access to HMIS.
- b. An individual whose background raises concerns about whether s/he may sufficiently be relied upon to help the HMIS Lead Agency achieve this goal may be enrolled as an HMIS End-user. After at least one year, if the individual demonstrates through proper and safe use of HMIS that the individual is reliable and trustworthy, they may apply to become a Technical Administrator.
- c. The results of the background check must be retained in the subject's personnel file by the Technical Administrator.
- d. A background check may be conducted only once for each person unless otherwise required

Establishing End-user Access

Licenses are given to prospective End-users only after they:

- a. Completes HMIS New User Orientation, which includes the Security and Ethics Training.

- b. Reads and understand the HMIS Policies and Procedures.
- c. Reads, understands, and signs the HMIS End User Code of Ethics.
- d. Reads and agrees to abide by the HMIS Agency Partnership Agreement.
- e. User must agree to comply with HMIS confidentiality practices.

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

- a. The End-user will be issued a unique User ID and password, which may not be transferred to one another. Instead, the Partner Agency will request an additional HMIS license, and if one is available, be issued a new User ID.
- b. The User IDs access level is granted based upon the End-user's job description.
- c. When an Agency Administrator determines a change to be made to user's access, s/he will notify the HMIS Lead.

End User's Access Levels

Five access levels exist in the HMIS system. Each level reflects the End-user's access to client-level records. Only agency staff who need access to the HMIS database for client data entry qualify for an End-user license. The level determines the type of information the End-user visualizes.

1. Agency Staff

- Access to data entry screens.
 - i. May access basic demographic data on clients (profile screen).
- Access to most TouchPoints.
- Full access to service records.
- Restricted access to reports.

2. Program Manager

- Access to all participant data screens.
- Restricted from administrative functions.
- Access to Touchpoints.
- Full access to reports.

3. Department Head

- Access to all features
- Access to some site-level administrative functions.
- Add/remove End-users for his/her Provider Agency.
- Edit some site and program data.
- Full reporting access.

4. Site Manager

- Access to all participant data features, including demographics, family data, and TouchPoints
- Access to site-level administrative functions.
 - i. Add/inactivate staff and program managers at site.
 - ii. Edit site program data.
 - iii. Full reporting access.

5. Enterprise Manager

- Access to HMIS for every Provider Agency.
- Access to enterprise administrative functions.
 - i. Setup new, modify and delete Provider Agencies/programs.
 - ii. Add new, modify, and activate/inactivate all users.
 - iii. Read and write access to all reports.
 - iv. Read and write access to all TouchPoints.
 - v. Access to all site management tools.
 - vi. Reset passwords.

Data Access & Password Policies

- a. The Agency Administrator contacts the HMIS Coordinator to set up a new End-user and provides a temporary password.
- b. The Agency Administrator communicates this password to the new End-user.
- c. The End-user must change the password after initially logging correctly into the database. Never transmit End-user identification and computer-generated passwords together in one email, fax, telephone call, or other means of communication. Passwords and usernames must be transmitted separately (e.g., one portion via email and the other via voice) unless physically handed to the End-user, who must destroy the paper transmission upon successfully entering the HMIS database
- d. The End-user creates a **unique** password between 8 and 16 characters with a minimum of two numbers. The End-user **DOES NOT** use a password used for other purposes; this password must be unique.
- e. Passwords shall not include the End-user name, the HMIS name, or the HMIS Vendor's name.
- f. Passwords should not consist entirely of any word found in the common dictionary or any of the above spelled backwards.
- g. Password is space and case sensitive.
- h. Passwords should be changed every 90 days.
- i. End-users must create a new password that is different from the original (expiring) password.

- h. Unique Passwords -- User IDs are individual, and passwords are confidential. No individual should ever use or allow the use of a User ID that is not assigned to that individual, and user-specified passwords should never be shared or communicated in any format.
- i. Protection of downloaded HMIS files:
Sonoma County Lead Agency assumes **no** responsibility for the management, protection, and transmission of client-identifying information stored on local agency computers, agency files, and reports.
 - 1. Partner Agency is responsible for any file or report downloaded from HMIS.

Rescind User Access

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

User access must be rescinded ASAP when:

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

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

Special Considerations

Termination or Extended Leave from Employment:

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

Virus Protection

- a. Sonoma County CoC HMIS Provider Agencies shall purchase and maintain state-of-the-art, commercially produced virus protection software, which includes automated scanning of files.

- b. Social Solutions Group shall maintain state-of-the-art, commercially produced virus protection software for the Sonoma County CoC HMIS server(s).
- c. At a minimum, any workstation accessing HMIS shall have antivirus software run the current virus definitions (24 hours), and full system scans a minimum of once per week.

Firewall

- a. Sonoma County CoC HMIS workstations shall maintain secure firewalls to protect against malicious intrusions. The firewall must be a part of a consistent overall Provider Agency security architecture.
- b. Social Solutions Group shall maintain secure firewalls for the Sonoma County CoC HMIS servers.

Disaster Recovery

The Disaster Recovery Plan for the Sonoma County HMIS will be conducted by the HMIS software Vendor, Social Solutions.

The Lead Security Officer should maintain ready access to the following information:

- a. Contact information – Phone number and email address of the Social Solutions contact responsible for recovering the agency's data after a disaster.
- b. Agency responsibilities – A thorough understanding of the Agency's role in facilitating recovery from a disaster.

The HMIS Coordinator(s) should be aware of and trained to complete any tasks or procedures for which they are responsible in the event of a disaster.

The HMIS Coordinator(s) must have a plan for restoring local computing capabilities and internet connectivity for the HMIS Coordinator(s)'s facilities. This plan should include the following provisions.

- a. Account information – Account numbers and contact information for the internet service provider and support contracts.
- b. Minimum equipment needs – A list of the computer and network equipment required to restore minimal access to the HMIS service, and to continue providing services to HMIS Partner Agencies.
- c. Network and system configuration information – Documentation of the configuration settings required to restore local user accounts and internet access.

Security Audits

The Contributory HMIS Organization (CHO) Security Officer/Participating Agency Security Officer is responsible for preventing degradation of the HMIS resulting from viruses, intrusion, or other factors within the Agency's control.

The participating Agency Security Officer is responsible for preventing inadvertent release of confidential client-specific information through physical, electronic, or visual access to the workstation.

Each participating Agency Security Officer is responsible for ensuring their agency meets the Privacy and Security requirements detailed in the HUD HMIS Data and Technical Standards. Partner Agencies will conduct a thorough review of internal policies and procedures regarding HMIS.

To promote the security of HMIS and the confidentiality of the data contained therein, access to HMIS will be available via a secure network.

End-users shall commit to abide by the governing principles.

Ongoing Monitoring

Agency Administrators conduct a security audit for all workstations that will use HMIS at least quarterly; this includes ensuring computers are protected by firewall and antivirus software.

The Agency Security Officers are responsible for managing the selection, development, implementation, and maintenance of security measures to protect HMIS information within their agency. At least quarterly, the Agency Security Officer will use the Compliance Certification Checklist to audit their workstations in the Agency. Should any Compliance Certification Checklist contain one or more findings, the finding will need to be resolved within seven days. The Agency Security Officer must turn in a copy of the Compliance Certification Checklist to the HMIS Lead Agency annually.

The HMIS Coordinator will visit each agency annually to evaluate each workstation's security using the Compliance Certification Checklist. Workstations will be assessed for noncompliance with standards or any element of Sonoma County's HMIS Policies and Procedures. The HMIS Coordinator will note these on the Compliance Certification Checklist and will work with the Agency Administrator to resolve the action item(s) within 30 days.

Enforcement Policies

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

- a. Affected agencies will make every attempt to resolve conflicts as they occur. The County and/or the Partner Agency may annotate their concerns in writing as appropriate.
- b. Unresolved conflicts between the Department of Health Services and a Partner Agency will be noted in writing and forwarded to the Department of Health Service's Ending Homelessness Manager. In the event of an impasse, members of the Data Committee will be notified within ten working days of the impasse declaration. Either party may declare an impasse.
- c. The Department of Health Service's Department of Health Service's Ending Homelessness Manager will review the written grievance and will make every attempt to resolve the matter within 30 days of review. Resolution of the conflict will be in writing and signed by all relevant parties.
- d. Unresolved conflicts will be forwarded to the Department of Health Service's Assistant Director for further guidance and action.
- e. Any recommendation regarding termination of a Partner Agency from Sonoma County's HMIS will be forwarded to the Department of Health Service's Assistant Director for consideration and possible action.
- f. All decisions of the Department of Health Service's Assistant Director are final.
 - Conflicts between or among Partner Agencies may require mediation by the Data Committee and/or HMIS Coordinator. Resolution of the conflict may be annotated in writing and signed by all relevant parties as appropriate.

HMIS Privacy Plan

These privacy policies establish limitations on the collection, purpose, and use of data. It defines allowable uses and disclosures, including standards for openness, access, correction, and accountability. Sonoma County's HMIS System focuses on enabling collaboration between partner agencies and supports an open data sharing structure. Demographic information may flow from partner agency to partner agency easily. Other HUD program-specific fields only flow once clients are enrolled in the new program if they were already part of the program. The policies provide protections for victims of domestic violence, dating violence, sexual assault, and stalking.

The HMIS Lead Agency is responsible for monitoring the partner agencies to ensure compliance with the Privacy Plan policies. The HMIS Coordinator will work with agencies not adhering to the Privacy plan and provide corrective measures for noncompliance.

Client Notification & Client Consent

- a. Partner Agency MUST

- Provide participant consent form(s) as required by the Partner Agency, state, and/or federal laws and the HMIS standards **prior** to entering client information into the HMIS database.
- Provide, in its original form or modified for the specific agency, the HMIS Client Release of Information for the Homeless Management Information System to permit the sharing of confidential client information to other HMIS Provider Agencies. Other non-HMIS inter-agency agreements do not cover the sharing of HMIS data.
- If a client elects not to complete the HMIS Client Release of Information, the partner agency can choose to complete an anonymous enrollment with de-identified client information into the HMIS database when that data is expected to be useful for organizing, providing, or evaluating the delivery of housing or housing-related services.
- A client signed Release of Information constitutes **INFORMED** consent. The burden rests with the Partner Agency End-user or intake counselor to inform the client about the purpose and function of HMIS data before asking for consent.
 - i. Any client receiving homeless services must fill out the Release of Information
 - ii. Any client participating in Coordinated Entry must fill out the CES Release of Information
 - iii. If clients do not feel comfortable providing their personal information into the HMIS, an option to choose an anonymous enrollment is provided. A signature will still be required, but the hard copy release will be stored with the agency outside of the HMIS system.
- As part of informed consent, a privacy notice must be posted in the intake area explaining:
 - i. the reasons for collecting the data,
 - ii. the client's rights with regards to data collection, and
 - iii. any potential future uses of the data.
- The agency must also make available the relevant Governance Policies & Procedures and a list of agencies participating in Sonoma County's HMIS Project.
- Be aware of specific protections afforded under Federal Law for persons receiving certain types of services such as domestic violence services, HIV or AIDS treatment, substance abuse services, or mental health services.
- Offer the client the opportunity to input and share additional client information with other Provider Agencies beyond basic identifying data and non-confidential service information.
- Obtain client consent for additional client information and communicate what information will be shared and with whom.

- Partner Agency End-users must obtain a new signed ROI and enter it into HMIS at project entry, or if the client's original release has expired; ROIs expire every two years.
- Data may be collected and entered into HMIS only when that data is expected to be useful for organizing, providing, or evaluating the delivery of housing or housing-related services.
- Data used for research or policy evaluation will be shared only after the data has been thoroughly de-identified; this includes removing names, contact information, and removing descriptions or combinations of characteristics that could be used to identify a person.
- Provide verbal explanation of Sonoma County CoC HMIS and arrange for, when possible, a qualified interpreter or translator for a client not literate in English or having difficulty understanding the consent form(s).
- End-users are prepared to explain (to the client) security measures used to maintain confidentiality.
- Participants' have the right to be entered as an anonymous client or as a restricted client. If the client denies authorization to share basic identifying information or non-confidential service data, follow the Anonymous Enrollment Document's steps.
- Prior to the release of any client information beyond the basic client profile, obtain from the client a signed release of information form that meets the Provider Agency's standard for the release of medical, financial and/or any other information regarding the client.
- Place all Client Release of Information forms in an onsite filing system for required recordkeeping standards and periodic audits.
- Retain all Client Release of Information forms for seven years upon expiration.
- Enter all minimum data required by the HMIS. Client data, including client identifiable and confidential information, may be restricted to other Provider Agencies. Each Agency Executive Director is responsible for their agency's internal compliance with the HUD HMIS Data Standards.

Provider Agency's Client Rights

A client has the right to:

- a. Decline to enter their record into the HMIS database.
- b. Authorize the sharing of personal information to other HMIS Provider Agencies.
- c. Determine what type of information will be shared and with whom (other HMIS Provider Agencies).
- d. Request entrance into the database as an anonymous client or a restricted client.

- e. Rescind acknowledgment and consent for the entry of future information and further participation.

Specific Client Notification for Victims of Domestic Violence

Victim service providers may not directly enter or provide client-level data to HMIS. Instead, a victim service provider, which is defined as a private nonprofit organization whose primary mission is to provide services to victims of domestic violence, dating violence, sexual assault or stalking, must use a comparable database that collects client-level data over time and generates unduplicated aggregate reports based on the data. Legal service providers may also elect to use a comparable database if it is necessary to protect attorney-client privileges. Victim Service Providers (VSP) in Sonoma County that receive funding requiring HMIS Data Entry utilize a comparable HMIS Data system to comply with requirements. VSPs have contracted with Social Solutions to provide their own copy of HMIS System. The system's use is restricted only to those employees with authority to view the data within the Victim Service Providers comparable HMIS system. Considering that ETO is the same system being used as the HMIS for Sonoma County, it is considered HUD compliant.

Privacy Compliance & Grievance Policy

Release and Disclosure of Client Data Policies

It is the primary governing principle of the Sonoma County HMIS that HMIS is intended to serve and protect the community's clients. Policies enacted to protect private client information are as follows.

- a. Clients shall be given a printout of all HMIS data relating to them upon written request within ten working days from the time the request is received. Written requests will be date/time stamped immediately upon receipt.
- b. A report of data sharing events, including dates, agencies, persons, and other details, must be made available to the client upon request within ten working days from the time the request is received. Written requests will be date/time stamped immediately upon receipt.
- c. A log of all external releases or disclosures must be maintained for seven years and made available to the client upon written request within ten working days from the time the request is received. Written requests will be date/time stamped immediately upon receipt.
- d. Aggregate data that does not contain any client-specific data may be shared with internal and external agents without specific permission. This policy should be made clear to clients as part of the informed consent procedure.

- e. Clients will be understood to be the owners of their own data. Each individual will have the right to grant informed consent, limit data sharing, or revoke consent related to his/her Protected Personal Information at any time.
- f. The community will encourage broad HMIS participation by human services agencies. HMIS End-users are expected to read, understand, and adhere to the spirit of these principles, even when the Policies and Procedures do not provide specific direction.

Resistance to Outside Disclosures

If an outside entity, such as a Court or law enforcement authority, attempts to access client-specific data, the outside entity will be politely but firmly instructed that the data is confidential and cannot be released without (i) a valid warrant, or (ii) the client's express consent. The client and/or the client's caseworker will then be informed of the attempted access so that the client can take any appropriate steps to resist any further attempts by outside parties to access their private information. No client-specific data will be released or shared outside of the Partner Agencies unless the client gives specific written permission or unless withholding that information would be illegal. Services may NOT be denied if the client refuses to sign Client Informed Consent and Release of Information Authorization or declines to state any information, but this may limit eligibility for certain programs in the Coordinated Entry System (e.g., permanent supportive housing).

Unauthorized Release of information

In emergency situations, i.e., security breach and/or imminent danger to the database, the HMIS Coordinator and the Ending Homelessness Manager have the final authority for the impending action for unauthorized releases of information.

In all other cases, the HMIS Coordinator implements a course of action outlined in the HMIS Partnership Violations and Termination – Data Transfer Policies sequence of procedures.

Corrective Action Plan Policy and Procedure

Policy: The Sonoma County CoC Homeless Management Information System (HMIS) Data Committee implements and maintains methods for correcting inappropriate database use.

Purpose: To establish guidelines and procedures to aid the HMIS Coordinator and HMIS staff in assisting Provider Agency's compliance with HMIS Policy and Procedures.

Scope: All Sonoma County CoC HMIS Staff and HMIS End-users

References: Maintenance of Client Confidentiality Monitoring Provider Agency Compliance

PROCEDURE:

HMIS Violation

Access and use of the HMIS database by HMIS Provider Agency staff and HMIS support staff is limited to the performance of their authorized job function. All other types of use are strictly forbidden and considered a Code of Ethics, Sonoma County CoC HMIS Policy and Procedures and/or the Agency Partnership Agreement security violation. The HMIS Coordinator may be contacted for clarification and guidance on possible HMIS violations.

Provider Agency Corrective Action Plan

- a. When an Agency Administrator becomes aware of a security violation within their agency, they will report the violation to the HMIS Coordinator immediately and provide the appropriate corrective action plan documentation.
- b. In the event of confirmed HMIS violation(s) by the Provider Agency or it's End-user(s), the HMIS Coordinator or appropriate HMIS staff member contacts the Provider Agency Executive Director or Agency Administrator and begins the Corrective Action Plan process

Corrective Action Plan Process:

HMIS Coordinator:

1. Contacts Provider Agency.
2. Identifies violation(s).
3. Provides references to the applicable HMIS Policy and Procedure.
4. Instructs Agency Administrator-Executive Director on how to fill out the Corrective Action Plan.
5. Identifies any HMIS training or resources that may assist in correcting issues.
Assists in coordinating a reasonable timeline.

Agency Administrator:

1. Fills out Corrective Action Plan.
2. Submits Corrective Action Plan within one week of notification via email or certified mail to HMIS Coordinator.
3. Contacts via phone and notifies the HMIS Coordinator.

HMIS Coordinator:

1. Acknowledges within 24 hours receipt of the Corrective Action Plan via email.
2. Reviews and determines feasibility of submitted Corrective Action Plan.

3. Contacts Provider Agency, within five working days, with any modifications to or approval of the submitted Corrective Action Plan.
4. Instructs HMIS staff to begin coordinating time-line dates and corrective changes into the monitoring procedure.

HMIS Staff:

1. Monitors the Corrective Action Plan.
2. Reports outcomes for each step in the Corrective Action Plan, on a weekly basis to the HMIS Coordinator.
3. Contacts immediately HMIS Coordinator of any further breaches of Policies and Procedures.

HMIS Coordinator:

1. Assesses corrective process and time-line adherence.
2. Reports to the Data Committee and SCDHS Ending Homelessness Manager areas of noncompliance.
3. Contacts the Provider Agency when Corrective Action Plan meets satisfactory completion or if further action will be taken (See Provider Agency Monitoring and Compliance Policy).

HMIS Staff:

1. Files completed report in Provider Agency file.

The Corrective Action Plan (see attachment) includes the following:

- Date of Notification
- Name of Provider Agency and End-user(s), when applicable
- Itemized specific violations
- A time frame for corrective measure(s) implementation and completion
- Itemized steps for corrective measures
- HMIS resources to be allocated: training, equipment, documents
- HMIS staff contact names, telephone numbers, and email addresses
- HMIS Coordinator phone number and email address

HMIS Coordinator and HMIS Staff Responsibilities:

- Monitor the corrective actions process for non-compliance issues and/or inappropriate actions.
- Identify further opportunities for improvement.
- Identify potential best practices.
- Assist in allocating HMIS resources and developing solutions for non-compliance issues, when possible.
- Maintain copies of correspondences and/or reports in the Provider Agency's file.
- Reviews and Corrective Action Plan Policy annually.
- Instructs HMIS Coordinator and HMIS Staff on development and implementation of additional monitoring reports and methodologies for identifying inappropriate actions.

Sonoma County HMIS Corrective Action Plan

Sonoma County Department of Health Services Homeless management Information System (HMIS) Corrective Action Plan

Agency: _____ Date of Notification: _____

Executive Director/HMIS Administrator: _____

Email: _____ Phone: _____

Itemized Violation(s)

Applicable Document(s)

- | | |
|----------|-------|
| 1. _____ | _____ |
| 2. _____ | _____ |
| 3. _____ | _____ |
| 4. _____ | _____ |

Itemized Corrective Measures

Expected Completion Date

- | | |
|----------|-------|
| 1. _____ | _____ |
| 2. _____ | _____ |
| 3. _____ | _____ |
| 4. _____ | _____ |

HMIS Resources

- | | |
|----------|----------|
| 1. _____ | 3. _____ |
| 2. _____ | 4. _____ |

Agency Administrator/Executive Director Signature

Date

Sonoma County HMIS Coordinator Signature

Date

HMIS Data Quality Plan

What is Data Quality?

Data Quality is the term that refers to the reliability, validity, and comprehensiveness of client-level data collected in HMIS. Good data quality represents reliable and valid data on persons accessing the homeless assistance system. With a strong data quality plan, multiple reports such as HUD Annual Performance Report (APR), Longitudinal System Analysis Report (LSA), and the Systems Performance Measure Report (SPMs) will be more accurate, and the HMIS coordinator will spend less time fixing errors. There are four main components to establish good data quality: timeliness, completeness, accuracy, and consistency.

Components of a Data Quality Plan

Timeliness

Entering data in a timely manner can reduce human error that occurs when too much time has elapsed between the data collection (or service transaction) and the data entry. The individual doing the data entry may be relying on handwritten notes or their own recall of a case management session, a service transaction, or a program exit date; therefore, the sooner the data is entered, the better chance the data will be correct. Timely data entry also ensures that the data is accessible when needed, either proactively (e.g., monitoring purposes, increasing awareness, meeting funded requirements) or reactively (e.g., responding to requests for information, responding to inaccurate information).

Sonoma County CoC HMIS Participating Agencies should adhere to entering client data into HMIS in a timely manner:

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

Completeness

Partially complete or missing data (e.g., missing digit(s) in an SSN, missing the year of birth, missing information on disability or veteran status) can negatively affect the ability to provide comprehensive care to clients. Missing data could mean the client does not receive needed services – services that could help them become permanently housed and end their episode of homelessness.

Sonoma County CoC HMIS goal is to collect 100% of all data elements. All agencies should strive to meet the goal of no more than five percent null/missing data (Data not collected, Client doesn't know, Client refused responses). However, it may not be possible in every situation depending on the data element and the type of program entering data.

In most cases, null, missing, "Data not collected", "Client doesn't know", "Client refused" responses are due to the client's understanding of the question. Asking clients if they understand the question or giving examples of how it is important to receive more funding based on the client's answer can help.

Accuracy

To ensure that the data that is collected and entered accurately. The accuracy of data in an HMIS can be challenging to assess. It depends on the client's ability to provide the correct data and the intake worker's ability to document and enter the data accurately.

Inaccurate data is worse than missing data, as this will not accurately reflect the client's journey through HMIS.

Some examples of data accuracy issues:

- Biological males as pregnant
- Minors as veterans
- Too many or not enough Heads of Household in any given household
- Congruency among the 3.917 Living Situation data elements
- Housing Move-In Date issues
- Destination issues, including "No exit interview completed" (what's accurate vs. what's missing/incomplete)
- Very low or very high bed utilization in a given period, based on beds available in the project (check for accuracy of client enrollments and exits from the project)
- Unaccompanied minors served by a project not serving the subpopulation.

Onsite monitoring can be used to monitor data accuracy by comparing paper files to data entered into HMIS:

- Does the information in the paper file match what is in HMIS?

- Is the information collection process done in such a way that it would encourage a high degree of accuracy?
- Intake staff can explain the data elements to clients in a clear, consistent, and accurate manner.
- The data collection process is conducted in a client-centered manner that includes privacy and building trust.

Additionally, the Longitudinal System Analysis Guide (see Appendix A in the LSA Guide) looks at specific data quality issues in relation to the system-wide submission to HUD on an annual basis. These specific data quality and data accuracy pieces should be addressed in the reports run by the HMIS Lead on an ongoing basis.

The Sonoma County CoC, in partnership with the HMIS Lead, will also work with providers to review, at regular intervals, the data collected directly from clients, either on paper forms or by being present during intakes with clients, and the data entered into HMIS to ensure that the data entered into HMIS matches the client's reality. This will be done, at a minimum, during annual formal onsite monitoring visits and will also occur at other points throughout the year.

Consistency

To ensure that data is understood, collected, and entered consistently across all programs in the HMIS. Consistency directly affects data accuracy; if an end-user collects all of the data, but they don't collect it in a consistent manner, the data may not be accurate.

End-users must share the same understanding of what each data element means, are trained in the same way, and given access to the same data entry guidance and training materials.

Monitor completeness by running DQ report weekly or bi-weekly to identify missing/refuse/don't know responses. In the cases where data quality is low, find the missing data or re-train case managers where needed.

Identifying and Correcting Errors in ETO HMIS

Data Quality Issues:

3.01 Name Quality of Name data is Client doesn't know, Client refused, Data not collected.	3.02 Social Security Social Security as it determines if it fits the SSN standards. <ul style="list-style-type: none">- Cannot contain a non-numeric character.- Must be 9 digits long- First three digits cannot be "000," "666," or in the 900 series.- The second group / 5th and 6th digits cannot be "00".- The third group / last four digits cannot be "0000".- There cannot be repetitive (e.g. "333333333") or
--	--

	sequential (e.g. “345678901” “987654321”) numbers for all 9 digits
3.03 Date of Birth Quality of Date of Birth data is Client doesn’t know, Client refused, or Data not collected	3.04 Race Race data is Client doesn’t know, Client refused, or Data not collected
3.05 Ethnicity Ethnicity data is Client doesn’t know, Client refused, or Data not collected	3.06 Gender Gender data is Client doesn’t know, Client refused, or Data not collected
3.07 Veteran Status <ul style="list-style-type: none"> • Veteran Status is Client doesn’t know, Client refused, Data not Collected 	3.08 Disabling Condition <ul style="list-style-type: none"> • Questions is: Client doesn’t know, Client refused, or Data not collected • At project start, there is a No for Disabling Condition, but one or more Disabling Condition are selected At project start, there is Yes for Disabling Condition, but no Disabling Condition are selected
3.10 Project Start Date Overlapping enrollments of the same project.	3.11 Project Exit Date Is prior to the Project Start Date
3.12 Destination Destination missing or has Client doesn’t know, Client refused, Data not Collected or has no exit interview completed	3.15 Relationship to Head of Household <ul style="list-style-type: none"> • Missing Head of Household OR • No Head of Household indicated on profiles OR More than one client is listed as the Head of Household
3.16 Client Location Data is missing or incomplete.	3.20 Housing Move-in Date Housing Move-in Date is blank for adults in Permanent Supportive Housing, Other Permanent Housing and Rapid Re-Housing projects
3.917 Prior Living Situation <ul style="list-style-type: none"> • Client Doesn’t Know, Client Refused, Data not collected for adults/HoH • Length of Stay is inconsistent with the prior living situation field. 	

Common Errors

- Systematic Errors/ Issues with Training
 - Entering “no” when you mean “yes”

- Definition drift
 - Entering text without using dropdown
 - Entering text without using dropdown
 - Random Errors/Sloppy Entry/Workflow
 - Date Errors (DOB is 4/15/52, entered 4/15/04)
- Transposing numbers
 - Spelling errors (Lauren vs. Loren)
 - Accidentally selecting the wrong response from a dropdown

Factors Impacting Quality

- Prioritized Process in the Organization?
- Are End-users given the time to participate in training and to complete entry?
- Is the environment arranged to support entry?
- Is the process owner within the Provider Agency respected?
- Is the data used?

Provider Agency Procedures for Ensuring Quality

- Standardized collection instruments
- Creating an environment conducive to data collection and entry
- Event triggers for data collection and entry – clearly defined workflow
- Guidance for special populations
- Must run reports monthly!

HMIS Bed Coverage

This section should address HMIS Bed Coverage and why it's important. It should talk through how the CoC and HMIS Lead can address bed coverage and what to do when new projects come online.

The importance of a high percentage of HMIS Bed Coverage for all project types is an emphasis of the HUD TA Data Strategy. Without a high percentage of HMIS Bed Coverage within a CoC, the data within HMIS is never holistic and the story told with HMIS data about homelessness within the CoC is never fully accurate. A lack of high HMIS Bed Coverage prevents CoCs from truly understanding how their system, and the clients served within their system, are functioning.

While extrapolation techniques can work for some research and reporting purposes, the extrapolation will only be as accurate as the similarities between any given projects, processes,

and clients served by the projects. Therefore, the goal for HMIS Bed Coverage for all project types is 100%.

The HMIS Lead, in conjunction with CoC Lead, will ensure that bed coverage is as close to 100% as is possible for all project types. This includes a review of the CoC's most recent Housing Inventory Chart (HIC) to know which providers participated in the most recent HIC but are not entering data into HMIS.

Ensuring a CoC's HMIS Bed Coverage reaches 100% and stays at 100% is a priority. This requires implementing a process to ensure new projects serving the at-risk/homeless population communicate with the CoC so that HMIS data entry can be encouraged and/or required for the new project.

Below are things to do to ensure HMIS Bed Coverage reaches or maintains at 100%:

- Review the HIC on a quarterly or semi-annual basis to ensure all projects (with the exception of Victim Services Providers) are entering data into HMIS;
- If projects are included on the most recent HIC that do not enter data into HMIS, the CoC and HMIS Lead should find out why this is the case and target any solutions to the specific "why";
- For any new project that becomes available within the CoC serving the at-risk/homeless populations, the CoC should be made aware and work with the HMIS Lead to ensure the new project is encouraged and/or required to enter data into HMIS.

Data Quality Training/ Performance Monitoring- HMIS

Sonoma County CoC HMIS Project Procedures for ensuring quality

1. HMIS staff reviews monthly reports for completeness, accuracy, and consistency.
2. Clear protocols for correcting data.
 - Provider Agency signs off on reports monthly
 - Errors systematically result in corrective action
 - Procedures for correcting are defined
3. Software has error checking functions (out of range, missing values, incongruous data).
4. Provider Agency staff looks at data reliability and validity issues before publishing reports. Collecting Provider Agencies will know which questions result in data that simply is not stable. Do the findings make sense? Must be knowledgeable about local services to recognize systematic data errors.

Deduplication of Data

Many HUD mandated reports ask for unique client counts. Duplication of client records can easily happen if the client's data is entered incorrectly or partially entered. Some common

examples include missing or incomplete social security numbers, misspelled names, or using an abbreviated name instead of using their full legal name. In cases such as these, two unique case numbers are created for the same individual.

When two unique client records are created for the same individual, one must choose the lower-case record number to be the “Primary” case number when merging the records. The Primary client record should be the case number that is the lowest; this allows the HMIS to track the length of time homeless for the client and helps with project eligibility (e.g., case number 123 would be chosen as the Primary over case number 1,456). The lower the case number is, the longer their homeless history is. System users must try to limit duplication of client records by adhering to the following responsibilities.

End-users will:

- Ensure basic demographic data is captured correctly (entering the full legal name, correct date of birth, and social security number if applicable).
- Use the search function prior to creating any new record; this includes searching the HMIS by name and their social security number if applicable).

Agency Administrator will:

- Merge duplicate client records when possible (the Provider Agency can only merge duplicates when both project enrollments are created within their HMIS projects).
- If the System Administrator cannot merge the duplicate client, the System Administrator will notify HMIS staff by email, including the two case numbers that require merging.

HMIS Coordinator/HMIS Staff will:

- Monitor possible duplication of records, at least every two weeks.
- Confirm the duplicate client id(s) with the Provider Agency requesting correct information (e.g., correct spelling of name or date of birth).
- Merge duplicate client records.

Technical Support

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

Support requests include reporting problems, requests for feature enhancements, or other general technical support. Under no circumstances should End-users submit support requests directly to the HMIS software vendor. The HMIS Lead Agency will only provide support for issues specific to HMIS software and systems.

User Training

HMIS Security and Ethics Training

A 30-minute Security and Ethics training is required for all staff working in the Sonoma County CoC HMIS. The training is offered before the start of New User Orientation and must be taken before starting to work in the system. A renewal training is also required annually by every staff person who comes into contact with Client protected information. End-user staff will contact the HMIS Coordinator to schedule this training either by phone or email.

HMIS New User Orientation

- HMIS Security and Ethics Training
- Overview of HUD HMIS Initiative
- Terminology
- Federal vs. local homeless funding and data collection rules
- Social Solutions

HMIS User Materials/Forms Website

- Assessments and Forms (Coordinated Entry and project level)
- Training Videos
- Homeless and At-Risk Definitions
- HMIS Policies and Procedures

Efforts To Outcomes (ETO) HMIS

- Login and User Security levels
- Screen tours
- Navigation
- Dashboards
- Workflows
- Metadata
- TouchPoint Assessment Entry
- Data Validations Reports

Agency/User Forms- <https://sonomacounty.ca.gov/health-and-human-services/health-services/divisions/homelessness-services/for-providers/sonoma-county-hmis>

Report Generation

HMIS Provider Database

The HMIS staff enters data into the HMIS Provider Database to produce reports on tracked areas. At a minimum, the reports include:

- Annual Performance Report (APR)
- Consolidated Annual Performance and Evaluation Report (CAPER)
- Data Quality Report
- Case Note Reports
- Rental Assistance History
- Days Between Estimated Date Homelessness Began and Program Start Date
- Exit Destinations in Period for HoHs Only
- HUD Assessment Timeliness
- Positive Exit Destinations and Housing Retention
- Quarterly Report
- Income Change for Project Leavers

HMIS staff with reporting level access can run reports on their own. If there are any issues with access, the HMIS Agency Administrator will contact the HMIS Coordinator to gain access to the needed report.

Provider Agency's Reporting Responsibilities

Laws and Regulations:

A Provider Agency will abide by:

- All Federal Confidentiality Regulations, including those contained in the Code of Federal Regulations, 42 CFR Part 2 (regarding disclosure of alcohol and/or drug abuse records).
- Health Insurance Portability and Accountability Act of 1996 (HIPAA) when applicable.
- California State and Federal laws related to confidentiality and security of medical, mental health, and substance abuse information including Code of Federal Regulations 42 CFR Part 2 and all other relevant statutes, rules, and regulations.

Report Preparation

A Provider Agency will:

- Retain access to all Provider Agency's client identifying and statistical data.
- Not report or release any identifiable client information on clients that the Provider Agency has not served or obtained a signed Consent to Release Information Form.

- Not report on any other Provider Agency's client data unless approved by that Provider Agency (See 2.0 for system-wide aggregate data).

Report Generation and Report Analysis

A Provider Agency will:

- Use database, standardized reports to maintain data integrity and perform business related duties.
- Use the HUD APR to report to HUD and upload CSV to Sage.
- Not manipulate data or statistics to defraud any person or organization.
- Only use database customized reports to inquire into another Provider Agency's data when it's essential to provide services to the client or determining eligibility.

System Wide Aggregate Date Procedure

System wide aggregate data:

- Includes client information from all Provider Agencies or a subset of Provider Agencies participating in the Sonoma County CoC HMIS.
- Does not include the HUD-APR and standardized reports.
- Does not apply to aggregate data produced by a Provider Agency that includes only that Provider Agency's data.

Creating System wide aggregate data

- Provider Agency may produce an aggregate in-house report using the Efforts To Outcomes (ETO) Web Intelligence Reporting System but cannot release the data or report without prior written permission from the Performance Measurement and Data Initiatives Task Group.
- Provider Agency asks and receives permission from the Data Committee through Custom Report Request Procedure.

Custom Report Request Procedure:

Provider Agency Duties:

- Fills out a Data Request Form (see Appendix)
- Submits brief explanation of reason for report requested and to whom the report will be released.
- Marks appropriate desired data elements
- Submits request to HMIS Coordinator

HMIS Coordinator Responsibilities:

- Checks report request for confidentiality and security breaches.

- Produces the requested report within 3-5 business days.
- **OR** returns Data Request Form to requesting Provider Agency with the reason the data elements violate confidentiality and security parameters. Provider Agency can work with HMIS Coordinator to modify report requested that adheres to confidentiality and security standards.

Publishing Requested Customized Data

- All Provider Agencies assume the sole responsibility for accurate data reporting and analysis to funding sources.

Community Data Requests (Non-HMIS Agencies/Organizations)

Reporting requests from non-participating HMIS organizations may be available at the discretion of the HMIS Lead Agency. The HMIS Lead Agency will evaluate factors including staffing capacity, current workload, and feasibility of each request prior to the approval or denial.

Local Changes to HMIS Policies & Procedures and other Documents

Changes to *HMIS Policies & Procedures*

1. Proposed changes may originate from any participant in a Partner Agency.
2. When proposed changes originate within a Partner Agency, they must be reviewed by the Partner Agency Executive Director and then submitted by the Partner Agency Executive Director to the HMIS Lead for review and discussion.
3. HMIS Lead Agency will maintain a list of proposed changes.
4. The list of proposed changes will be discussed by the Data Committee, subject to line-item excision and modification. This discussion may occur either at a meeting of the group, via email or conference call, according to the discretion and direction of the group.
5. Once proposed changes have been approved by the Data Committee with a majority vote in favor, revisions to the HMIS Policies and Procedures will be submitted to the CoC Board for final approval.
6. Within ten working days after approval by the CoC Board, the HMIS Lead Agency will forward a copy of the adopted HMIS plans, forms, standards and/or governance documents to all HMIS Partner Agency Executive Directors.
7. Partner Agencies Executive Directors shall acknowledge receipt and acceptance of the revised *HMIS Policies and Procedures* within ten working days of delivery of the amended *HMIS Policies and Procedures* by notification in writing or email to HMIS Lead Agency. Partner Agency Executive Director shall also ensure circulation of the revised document within their agency and compliance with the revised *Governance Policies and Procedures*.

Other Obligations and Agreements

Current funding for HMIS provides for a limited number of software End-user licenses. While it may not be possible to meet every Partner Agency's requests for End-user licenses within the existing funding, the HMIS Lead Agency, in partnership with the Continuum of Care, will endeavor to ensure that every Partner Agency will have its minimum requirements met.

Participation fees are based on a number of different factors such as a flat rate fee, HMIS license counts, bed capacity, the number of clients served and the data quality of the program.

Forms Control

All forms edits and changes required by these Policy and Procedures are available from the HMIS Lead Agency. All documents of the Policy and Procedures, Security Plan, Privacy Plan, Privacy Policy and Data Quality Plan and forms will be reviewed annually.

Development and Maintenance of Required HMIS Policies and Standards

The HMIS Lead must develop new policies annually to remain in compliance with changes in Coordinated Entry Guidance, HMIS Data Standards and any new regulations. Additionally, the HMIS Lead Agency must review and update existing Documents including the Privacy Plan, Data Quality Plan, Security Plan, Governance Charter & Policies and Procedures at least annually. While the final responsibility resides with the HMIS Lead Agency, Sonoma County divides the duties between 3 parties, The Data Committee, the HMIS Lead Agency, and the Sonoma County Homeless Coalition Board.

Responsibilities:

1. The HMIS Lead Agency is responsible for updates to the HMIS Policies and Procedures, the creation of or any revisions to existing documents for HMIS in compliance with new regulations and system changes.
2. The Data Committee will review, provide feedback and approve any HMIS procedural and/or document changes.
3. The Sonoma County Homeless Coalition Board will have final approval of annual revisions to the HMIS Policies and Procedures.

As new funding initiatives are established by federal, state, and local government as well as private philanthropy, the list of programs whose performance is monitored by Sonoma County Homeless Coalition Board will grow.

Glossary of Terms

1. *Anonymous client*: A client entered into the database with a unique computer-generated identifying code acting as a reference for that client.
2. *Client*: Any person who received, applied for or was denied services by a Provider Agency.
3. *Client Identifying Information*: Any information or a combination of data that would allow an individual client to be identified including but not limited to name, nick name, social security number, military identification number, health insurance carrier number.
4. *Client's guardian*: Any person legally responsible for a minor or an adult, according to California Revised Statutes (A.R.S.). All references to "client" in this policy also apply to "client's guardian."
5. *Close to real-time*: Data entry within one business day.
6. *Computer virus*: A self-replicating piece of computer code, which resides in active memory and partially or fully, attaches itself to files and/or applications.
7. *Consultation*: A discussion, usually by phone, reminding the End-user or Provider Agency, of proper security and/or confidentiality practices(s), following confirmed inappropriate action(s).
8. *Custom Report*: A report, which can be created by HMIS Provider Agencies using *ETO Results*.
9. *Efforts To Outcomes*: A web-based information management system for service providers of an agency, coalition or region of any size which provides client tracking, case management, agency and program indexing, and reporting – all in a real-time environment.
10. *End-user*: Any person given access to the database including staff and volunteers.
11. *Error*: A documentable occurrence that prevents an end-user from proceeding further.
12. *Firewall*: A system or group of systems that enforces an access control policy between two networks. The system may contain a pair of mechanisms: one that exists to block Internet traffic, and the other that exists to permit Internet traffic.
13. *HMIS Lead*: Agency-designated lead in overseeing training, data input and validation at each HMIS participating agency.

14. *HMIS Provider Database*: A software application, which allows HMIS staff to track all communication relating to Provider Agencies.
15. *Malicious code*: An illegitimate computer code, which produces an undesired effect including, viruses and worms.
16. *Outside source(s)*: Organization(s) who are not current HMIS Provider Agencies.
17. *Performance*: The execution and/or operation of the software, or lack thereof.
18. *Probation*: A trial period of time, not greater than one hundred and eighty days (180), in which an End-user or Provider Agency addresses and corrects inappropriate actions(s).
19. *Provider Agency*: An agency authorized to participate in the Sonoma County Homeless Management Information System.
20. *Quality of Data Issue*: Any concern that decreases the accuracy and completeness of the data as defined by the Minimum Data Requirement.
21. *Real-time*: Immediate data entry upon seeing a client.
22. *Reinstatement Corrective Action Plan*: A modified Corrective Action Plan developed specifically for the purpose of preparing and assessing the appropriateness of reinstating a previously terminated Agency as an HMIS Provider Agency.
23. *Restricted client*: A client whose name is known by only the entering Provider Agency, HMIS Coordinator, and those agencies to whom the client grants access to his/her name.
24. *Sanctions*: Penalties for noncompliance specified by the HMIS Data Policy Group.
25. *Suspension*: An act of postponing database access, after an End-user or Provider Agency receives written notice via certified mail explaining a breach of contract, quality of data issue or improper security and/or confidentiality practices, where the guilty party received previous warning(s) and did not correct inappropriate actions.
26. *Technical Support Staff*: Include, in ascending order, site HMIS Lead, Sonoma County HMIS Coordinator, and Social Solution Group's (SSG) Help desk personnel.
27. *Termination*: The act of ending database access, after an End-user or Provider Agency receives an appropriate written notice via certified mail explaining the reasons for cessation of database use.
28. *Written Warning*: A printed notice informing the End-user or Provider Agency of a confirmed inappropriate action and a corrective explanation.