HOMELESS RESOURCE COUNCIL OF THE SIERRAS

HMIS POLICIES AND PROCEDURES MANUAL

January 2018

Contents

EXHIBITS

Attachments

SECTION 1: HMIS OVERVIEW

Definition of Homeless Management Information System (HMIS)

A Homeless Management Information System (HMIS) is a locally administered electronic data collection tool used to record and store client-level information about the numbers, characteristics, and needs of persons who use homeless housing and supportive services or homelessness prevention services.

HMIS is essential to efforts to coordinate client services and inform community planning and public policy. Through HMIS, homeless individuals benefit from improved coordination within and among agencies, informed advocacy efforts, and policies that result in targeted services. Analysis of information gathered through HMIS is critical to the preparation of a periodic accounting of homelessness in Homeless Resource Council of the Sierras region, including required US Department of Housing and Urban Development (HUD) reporting.

HUD HMIS Requirement

Since 2004, HUD has required recipients of Continuum of Care (CoC) Program funds to collect electronic data on their homeless clients in HMIS. HUD published HMIS Data and Technical Standards in the Federal Register in 2004. HUD has since amended the HMIS Data Standards. In 2011, HUD published a proposed rule establishing HMIS requirements (76 FR 76917). The proposed rule requires that every CoC have an HMIS that is operated in compliance with the requirements of 24 CFR part 580.

Homeless Resource Council of the Sierras' HMIS: HMIS Lead and System

The Homeless Resource Council of the Sierras (HRCS), the Nevada and Placer Counties CoC, has been designated as the CoC's HMIS Lead Agency. The Homeless Resource Council of the Sierras' will designate a full-time HMIS Administrator to both assure the quality of data entered in the database and to support general usage by all projects using the system. The HMIS Administrator is also responsible for structural changes to the database to capture information, for developing necessary reports, and for overseeing privacy and security policies. The HMIS Administrator reports to the HRCS who is responsible for approving all policy decisions made by the CoC.

The CoC has selected Mediware ServicePoint software to serve as the CoC's HMIS. Each Contributing HMIS Organization (CHO) has its own agency and project sites within the software. ServicePoint serves as a web-based direct data entry portal for organizations that use ServicePoint as their data management system. ServicePoint also serves as a Data Warehouse for the Homeless Resource Council of the Sierras, enabling participating agencies to upload data to the Data Warehouse, so long as those systems meet all applicable HUD and CoC HMIS requirements as outlined in these policies and procedures.

ServicePoint meets all Health Insurance Portability and Accountability Act (HIPAA) standards for security, privacy and confidentiality.

Contributing HMIS Organizations (CHOs)

All Homeless Resource Council of the Sierras' recipients of grants from programs authorized by Title IV of the McKinney-Vento Act are required to contribute data to the CoC's HMIS, with the exception of victim service providers and providers of legal services. In addition, all other Homeless Resource Council of the Sierras' agencies that provide shelter, housing and services to homeless and at risk populations are encouraged to use the Homeless Resource Council of the Sierras' HMIS database.

An agency that participates in HMIS, referred to as a CHO, must execute a Participation Agreement with the HMIS Lead and must agree to abide by the policies and procedures outlined in this document. CHOs oversee and are responsible for their client level data, are responsible for the integrity and security of their agency's client level data, and assume the liability for any misuse of the system by agency staff. Participating agencies are responsible for ensuring that their agency users comply with the policies and procedures outlined in this manual.

Governance

The Homeless Resource Council of the Sierras adopted an HMIS Governance Agreement in September 2013, which defines the roles and responsibilities of the CoC, the HMIS Lead, CHOs, and the CoC HMIS Committee. These HMIS Policies and Procedures incorporate the terms of the HMIS Governance Agreement.

Definitions of Key Terms

The section below defines key terms used throughout this document and HUD guidance regarding HMIS.

Comparable Database	A database that is not the CoC's official HMIS, but an alternative system that victim service providers and legal services providers may use to collect client-level data over time and to generate unduplicated aggregate reports based on the data, and that complies with the requirements of this part. Information entered into a comparable database must not be entered directly into or provided to an HMIS.
Continuum of Care (CoC)	The group composed of representatives from organizations including nonprofit homeless providers, victim service providers, faith-based organizations, governments, businesses, advocates, public housing agencies, school districts, social service providers, mental health agencies, hospitals, universities, affordable housing developers, law enforcement, organizations that serve veterans, and homeless and formerly homeless persons organized to carry out the responsibilities of a Continuum of Care established under 24 CFR part 578.
Contributory HMIS Organization (CHO)	An organization that operates a project that contributes data to an HMIS.
Homeless Management Information System	The information system designated by Continuums of Care to comply with the requirements of 24 CFR part 580 and used to record, analyze, and transmit client and activity data in regard to the provision of shelter, housing, and services to individuals and families who are homeless or at risk of homelessness.

[1] Victim services providers are prohibited from entering client data into HMIS and must instead enter required data into a comparable database. Legal services providers are not prohibited from entering client-level data into HMIS, but may elect to use a comparable database instead of the HMIS, if the data is protected by attorney-client privilege.

HMIS Lead	The entity designated by the Continuum of Care in accordance with 24 CFR part 580 to operate the Continuum's HMIS on its behalf. The HMIS Lead is the the Homeless Resource Council of the Sierras.
HMIS Vendor	A contractor who provides materials or services for the operation of an HMIS. An HMIS vendor includes an HMIS software provider, web server host, data warehouse provider, as well as a provider of other information technology or support. The HMIS Vendor for the Homeless Resource Council of the Sierras is Bowman Systems, LLC.
Protected Personal Information (PPI)	Information about a project participant that can be used to distinguish or trace a project participant's identity, either alone or when combined with other personal or identifying information, using methods reasonably likely to be used, which is linkable to the project participant.
User	An individual who uses or enters data in an HMIS or another administrative database from which data is periodically provided to an HMIS.
Victim Services Provider	A private nonprofit organization whose primary mission is to provide services to victims of domestic violence, dating violence, sexual assault, or stalking. This term includes rape crisis centers, battered women's shelters, domestic violence transitional housing projects, and other projects.

Policy Review and Amendment

The Homeless Resource Council of the Sierras' HMIS policies and procedures must comply with HUD regulations and/or technological changes. The HMIS Lead will review the policies and procedures annually and at the time of any change to the system management process, the data warehouse software, the methods of data exchange, or any HMIS data or technical requirements issued by HUD.

In the event that changes are required to the HMIS policies and procedures, the HMIS Lead will develop recommendations to the HMIS Committee for review, modification, and approval. The HMIS Committee will present the Board of Directors with recommended changes to the policies and procedures, and the new policies and procedures will be reviewed, modified, and voted on by the Board of Directors. The HMIS Lead will modify practices, documentation, and training material to be consistent with the revised policies and procedures within six months of approval.

Privacy, Security and Data Quality Plans

The HMIS Lead, in consultation with CHOs and the CoC, is responsible for creation and updating of Privacy, Security, and Data Quality Plans which conform to HUD requirements. These Plans are incorporated into these policies and procedures, and must be complied with by the HMIS Lead and all CHOs.

SECTION 2: PARTICIPATION IN HMIS

Contribution of Data

Data is contributed directly to the Homeless Resource Council of the Sierras' HMIS. Agencies that contribute directly are provided web-based log-in information with which to access the system.

All contributors are subject to all relevant Homeless Resource Council of the Sierras' HMIS policies and procedures.

Participation Agreement

All CHOs that participate in the Homeless Resource Council of the Sierras' HMIS must sign and agree to abide by the terms of the Participation Agreement, the contract between the CHO and the HMIS Lead.

The Homeless Resource Council of the Sierras' HMIS Administrator will maintain files for all CHOs. CHO files will include, but are not limited to, Participation Agreement (Attachment 1), all End User Agreements (Attachment 2), all Security Officer Declarations (Attachment 3), all CHO Security Certifications (Attachment 4), current Authorized User List (Attachment 5), all User Account/Termination Request forms (Attachment 6), all CHO Profile forms (Attachment 7), and any other documents pertaining to the CHO's participation in the HMIS.

CHO HMIS Site Manager/Security Officer

Each CHO must designate a single agency representative to act as the CHO's HMIS Site Manager/Security Officer. CHO HMIS Site Managers are responsible for the following:

- Communicate personnel for HMIS users to the Homeless Resource Council of the Sierras' HMIS Administrator;
- Act as the first tier of support for agency HMIS users;
- Act as the liaison or contact between the agency and Homeless Resource Council of the Sierras' HMIS Administrator;
- Ensure that the agency adheres to client privacy, confidentiality, and security policies;
- Maintain compliance with technical requirements for participation;
- Ensure that the Privacy Notice is being used;
- Enforce data collection, entry, and quality standards; and
- Attend quarterly HMIS Committee meetings.

Technological Requirements for Participation

All computers accessing the Homeless Resource Council of the Sierras' HMIS on behalf of the agency must meet the minimum system requirements as outlined in the HMIS Security Plan.

Prior to granting a user access for any staff member, the CHO HMIS Site Manager/Security Officer will assess the operational security of the user's workstation.

CHO Profiles in HMIS

Each agency must be set up in HMIS, with profiles that define the projects and services the agency offers, prior to HMIS use and data entry. CHOs should contact the Homeless Resource Council of the Sierras' HMIS Administrator for agency set up. CHO Profiles will be reviewed and updated on an annual basis.

Authorization of HMIS Users; Access to HMIS

Only authorized individuals that have completed the necessary privacy, security, and data entry training and have signed and submitted the HMIS CHO End User Agreement will be provided a username and password and allowed to access HMIS on behalf of their agency.

To add a new agency HMIS User, a CHO must submit a completed copy of the HMIS User Account Request/Termination Form to the Homeless Resource Council of the Sierras HMIS Administrator. Each CHO HMIS Site Manager should keep an updated Authorized User List of approved agency users; this document should be submitted to the Homeless Resource Council of the Sierras' HMIS Administrator upon any changes to authorized users.

The HMIS Administrator will provide each new HMIS User with a unique user name and password. The HMIS User must change the password the first time he/she logs into the system.

Training

All new End Users must receive training prior to receiving their username and password. Training will include Security, Privacy, Data Standards, and Data Entry. The training is scheduled as needed to accommodate new users and agencies.

All End Users must attend an annual training to review all Security, Privacy, Data Standards, and Data Entry protocols. The Annual Training will be scheduled every 6 months and may also be scheduled as needed if the user is unable to attend one of the regularly scheduled training. (Each user is only required to attend one review training each year.)

Data Collection Training is available for CHO's employees that are involved in the data collection and data entry process. The training will be scheduled as needed to accommodate the different agencies' schedules.

Report Writer training is provided on an as needed basis.

Basic ART training may be scheduled with the HMIS Lead Agency, but intermediate or advance training for ART will be at the expense of the requesting agency and will be administered by Bowman Systems, LLC.

End User Agreements

A Homeless Resource Council of the Sierras' HMIS CHO End User Agreement must be signed and kept for all agency personnel or volunteers that will access HMIS data on behalf of the agency. Agencies must store copies of all Homeless Resource Council of the Sierras' HMIS CHO End User Agreement for at least five (5) years. Agencies should never dispose of their copy of the Homeless Resource Council of the Sierras' HMIS CHO End User Agreement upon revoking an individual's authorization or in terminating an individual's employment.

CHO Site Managers must forward the signed Homeless Resource Council of the Sierras' HMIS CHO End User Agreement to the HMIS Administrator.

Removing Authorized Personnel

The Homeless Resource Council of the Sierras' HMIS System Administrator must be notified by phone or email within one business day when an individual is no longer authorized to access HMIS on the agency's behalf. CHOs must follow up by sending a completed HMIS User Account Request/Termination Form via email or fax to the HMIS System Administrator. When a CHO provides an HMIS User Account

Request/Termination Form to the Homeless Resource Council of the Sierras' HMIS System Administrator, it must also provide an updated Authorized User List. Upon receipt of the request, the Homeless Resource Council of the Sierras' HMIS System Administrator will immediately deactivate the individuals' HMIS user account.

SECTION 3: DATA COLLECTION AND DATA QUALITY

Collection of Data on Participants and Non-Participants

Agencies should collect data from families and individuals who are homeless or at risk of becoming homeless and are accessing services from their agency. Agencies may also choose to collect data for HMIS on individuals or families that make contact with the agency, but are not able to receive services from the agency. Information must be collected separately for each family member, and all family member data must be entered into the database.

A current HMIS Client Release of Information (Attachment 8) form must be kept by the agency entering the client's information.

Required Data Elements

The HMIS Data Standards outline three categories of required data elements. Two of these categories are at the client level and the third, Project Descriptor, is at the project level.

HUD Universal Data Elements:

Universal Data Elements (UDEs) are to be collected from all clients served by all homeless assistance projects reporting to the HMIS. The Universal data elements are: Name, Social Security Number, Date of Birth, Race, Ethnicity, Gender, Veteran Status, Disabling Condition, Residence Prior to Project Entry, Project Entry Date, Project Exit Date, Destination, Personal ID, Household ID, Relationship to Head of Household, Client Location, and Length of Time on Street, in an Emergency Shelter, or Safe Have. ServicePoint automatically generates the unique person identification number, the project identification number and household identification number data elements.

HUD Project Specific Data Elements:

Project Specific Data Elements (PSDEs), as defined in the HMIS Data Standards, are data elements that are required for projects receiving certain types of funding, but are optional for other projects. Project specific data elements are necessary to complete Annual Progress Reports (APRs) required by projects that receive funding under the McKinney-Vento Homeless Assistance Act. Refer to the 2014 HMIS Data Standards for a complete list of Project Specific Data Elements.

Project Descriptor Data Elements

The Project Descriptor Data Elements (PDDEs) are required of all projects in a Continuum of Care and provide descriptive information about an agency and their projects. The HMIS Lead collects Project Descriptor Data Elements and updates these elements on all projects annually. Refer to the 2014 HMIS Data Dictionary for a list of Project Descriptor Data Elements.

HMIS Data Collection Standards and Assessments

Timeliness and Project Entry and Exit Dates

Agencies may choose to enter data directly into the HMIS or to collect client level data on paper prior to entering into HMIS. If agencies use paper data collection forms, all hard copy forms and services must be entered into the database within one (1) week. Whether direct data entry or paper forms are used the data collected and entered must be consistent with the data provided by the client and the hard copy data collection form the project uses.

IMPORTANT: Data entry and exit dates entered into HMIS must reflect actual dates that the participant entered and exited the project, not the date of data entry or update.

Intake, Assessment and Exit Forms

There are templates of forms that may be adopted or adapted by CHOs for data collection including, but not limited to: HRCS HMIS Entry Forms, HRCS HMIS Update Forms, HRCS HMIS Annual Assessment Forms, HRCS HMIS Exit Forms, HRCS HMIS Referral Tracking and Contact Tracking Forms. If information is being collected on a family, information must be collected on each member of the family.

Client Intake and Initial Assessment

Client Intake is the process of collecting and then entering new client data or updating existing information for a client that is already in HMIS. Every agency should enter and/or update the Universal Data Elements for all household members upon intake. Agencies which collect Assessment data must also collect this on each household member at project entry/intake. Where a client already has a record in HMIS, Client Intake requires updating all client information as of the intake date.

Interim/Update Assessments

Ongoing assessments and updating of participant information enables the project and the CoC to assess progress toward housing stability, increased income, and increased access to mainstream benefits. Continuum of Care projects must complete annual assessments for all participants at least once per year within 30 days of the clients' anniversary date into the project. Emergency Solutions Grant projects must complete interim/update assessments for all participants when information changes AND at least every 3 months for Homelessness Prevention AND at least annually for Rapid Rehousing. All other projects entering data into the HMIS must complete an update whenever there is a change in client information (e.g. Increased Income, Receiving Mainstream benefits, etc.).

Project Exit Assessment

The Exit Assessment provides information on the participant's status at exit, as well as the participant's housing destination. An exit assessment must be completed for all exiting participants.

Data Quality

The value of HMIS depends on the quality of the data entered into the project. All projects must strive to provide the most accurate and consistent data as is possible.

Reducing Duplicates

Users should ensure that duplicate records are not created within ServicePoint by conducting a thorough client search at intake. If duplicates are created, the CHO must work with the HMIS Lead to merge the duplicate records.

Improving Data Quality

All CHOs must comply with standards set forth in the Homeless Resource Council of the Sierras' HMIS Data Quality Plan, which is incorporated into these policies and procedures.

SECTION 4: COMPLIANCE, TECHNICAL ASSISTANCE, & SANCTIONS

The goal of the CoC and the HMIS Lead is to ensure that all CHOs are in compliance with all requirements and are using the HMIS to improve services to participants.

Compliance and Technical Assistance

CHOs are required to comply with these policies and procedures, and with the CoC's HMIS Privacy, Security, and Data Quality Plans. Where CHOs have difficulty achieving compliance, the HMIS Lead will provide technical assistance. The CHO may request technical assistance, or the HMIS Lead may offer it.

CHOs are subject to annual HMIS monitoring. Where compliance issues are identified through monitoring or become apparent between monitoring, the HMIS Lead will request that the CHO provide a plan for coming into compliance, and the HMIS Lead will monitor progress toward meeting requirements of the plan.

Availability of Sanctions

In the event of violations of privacy or confidentiality standards, or ongoing failure to meet data quality standards, sanctions may be warranted.

Potential sanctions include the following:

- Required to retake a training course;
- Suspending or terminating agency access to the HMIS;
- Suspending or terminating user access to the HMIS;
- Mandatory training prior to reinstatement to the HMIS.

Sanctions Procedure

Sanctions may only be imposed by the HRCS Board of Directors. An initial recommendation that sanctions be imposed is generated by the HMIS Lead, and is presented to the HRCS Board regarding specific sanctions to be imposed. The Board may impose the recommended sanction, or a different sanction that it believes is appropriate.

Sanctions Separate from Project Review for Renewal

Each CHO's record of compliance with the policies and procedures set forth in this Manual and the level of data quality achieved will be reported to the CoC Application Committee, which may take these factors into consideration in determining which projects will be submitted for renewal, and which agencies may be permitted to apply for new project funding. Decisions of the CoC Application Committee are separate and distinct from decisions concerning imposition of sanctions.

Homeless Resource Council of the Sierras’ HMIS

SECURITY PLAN

Security Officers

The Homeless Resource Council of the Sierras’ Homeless Management Information System (HMIS) Lead Agency (herein referred to as the HMIS Lead Agency), has designated an HMIS Security Officer whose duties include:

- Review of the Security Plan annually and at the time of any change to the security management process, the data warehouse software, the methods of data exchange, and any HMIS data or technical requirements issued by HUD. In the event that changes are required to the HMIS Security Plan, the Security Officer will work with the HMIS for review, modification, and approval.
- Confirmation that the HMIS Lead Agency adheres to the Security Plan.
- Response to any security questions, requests, or security breaches to the Homeless Resource Council of the Sierras’ HMIS and communication of security-related HMIS information to CHOs.

Each Contributing HMIS Organization must also designate a CHO Security Officer whose duties include:

- Confirmation that the CHO adheres to the Security Plan.
- Communication of any security questions, requests, or security breaches to the Homeless Resource Council of the Sierras’ HMIS Security Officer, and security-related HMIS information relayed from the Homeless Resource Council of the Sierras’ HMIS System Administrator to the CHO’s end users.
- Participate in security training offered by The HMIS Lead Agency.

Annual Security Certification

The HMIS Lead Agency and each CHO must complete an annual security review to ensure the implementation of the security requirements for the HMIS. This security review must include completion of a security checklist ensuring that each of the security standards is implemented in accordance with the HMIS security plan. Each CHO Security Officer must complete the CHO Security Certification each January using the attached form and submit the completed form to the HMIS Security Officer no later than February 15 of each year.

Security awareness training and follow-up

All users must receive security training prior to being given access to the HMIS. The HMIS Lead Agency shall provide security training no less than once per year.

Reporting security incidents

The HMIS Lead has created the following policy and chain of communication for reporting and responding to security incidents.

Security Incidents

All HMIS users are obligated to report to their agency HMIS Security Officer suspected instances of noncompliance with policies and procedures that may leave HMIS data vulnerable to intrusion. Each CHO is responsible for reporting any security incidents involving the real or potential intrusion of the

Homeless Resource Council of the Sierras' HMIS to HMIS Lead Agency. HMIS Lead Agency is responsible for reporting any security incidents involving the real or potential intrusion of the Homeless Resource Council of the Sierras' HMIS to the Homeless Resource Council of the Sierras Board.

Reporting Threshold

HMIS users must report any incident in which unauthorized use or disclosure of Protected Personal Information (PPI) has occurred and any incident in which PPI may have been used in a manner inconsistent with the HMIS Privacy or Security Policies. Security breaches that have the possibility to impact the Homeless Resource Council of the Sierras' HMIS must be reported to the HMIS System Administrator.

Reporting Process

HMIS users will report security violations to their CHO Security Officer. The CHO Security Officer will report violations to HMIS Security Officer. Any security breaches identified by Bowman Systems, LLC will be communicated to HMIS Security Officer. The HMIS Security Officer will review the violation with the HMIS Administrator. The HMIS Administrator will recommend corrective and disciplinary actions to the HMIS Committee and the Homeless Council of the Sierras Board, as appropriate. Each CHO will maintain and follow procedures related to internal reporting of security incidents.

Audit Controls

Bowman Systems, LLC maintains an accessible audit trail within ServicePoint that allows the Homeless Resource Council of the Sierras' HMIS System Administrator to monitor user activity and examine data access for specified users. The Homeless Resource Council of the Sierras' HMIS Administrator will monitor audit reports for any apparent security breaches or behavior inconsistent with the Privacy Policy outlined in the policies and procedures.

System Security

Each CHO must apply system security provisions to all the systems where personal protected information is stored, including, but not limited to, a CHO's networks, desktops, laptops, mini- computers, mainframes and servers.

User Authentication

A CHO must secure HMIS ~~systems~~ with, at a minimum, a user authentication system consisting of a username and a password. Passwords must be at least eight characters long and meet reasonable industry standard requirements.

Using default passwords on initial entry into the HMIS application is allowed so long as the application requires that the default password be changed on first use. Written information specifically pertaining to user access (e.g., username and password) may not be stored or displayed in any publicly accessible location. Individual users must not be able to log on to ServicePoint from more than one workstation or location at a time.

Virus Protection

A CHO must protect HMIS ~~systems~~ from viruses by using commercially available virus protection software. Virus protection must include automated scanning of files as they are accessed by users on the system where the HMIS application is housed. A CHO must regularly update virus definitions from the software vendor.

Firewalls

A CHO must protect HMIS ~~systems~~ from malicious intrusion behind a secure firewall. Each individual workstation does not need its own firewall, as long as there is a firewall between that workstation and any systems, including the Internet and other computer networks, located outside of the organization. For example, a workstation that accesses the Internet through a modem would need its own firewall. A workstation that accesses the Internet through a central server would not need a firewall as long as the server has a firewall.

Physical Access to Systems with Access to HMIS Data

A CHO must staff computers stationed in public areas that are used to collect and store HMIS data at all times. When workstations are not in use and staff is not present, steps should be taken to ensure that computers and data are secure and not usable by unauthorized individuals. After a short amount of time, workstations should automatically turn on a password protected screen saver when the workstation is temporarily not in use. If staff from a CHO will be gone for an extended period of time, staff should log off the data entry system and shut down the computer.

Hard Copy Security

A CHO must secure any paper or other hard copy containing personal protected information that is either generated by or for HMIS, including, but not limited to, reports, data entry forms and signed consent forms. A CHO must supervise at all times any paper or other hard copy generated by or for HMIS that contains PPI when the hard copy is in a public area. When CHO staff is not present, the information must be secured in areas that are not publicly accessible.

Hard copies of data stored or intended to be stored in HMIS, regardless of whether the data has yet been entered into HMIS, will be treated in the following manner:

1. Records shall be kept in individual locked files or in rooms that are locked when not in use.
2. When in use, records shall be maintained in such a manner as to prevent exposure of PPI to anyone other than the user directly utilizing the record.
3. Employees shall not remove records or other information from their places of business without permission from appropriate supervisory staff unless the employee is performing a function which requires the use of such records outside of the CHO’s place of business and where return of the records by the close of business of would result in the undue burden on staff.
4. When staff remove records from their places of business, the records shall be maintained in a secure location and staff must not re-disclose the PPI contained in those records except as permitted by these policies and procedures.
5. Faxes or other printed documents containing PPI shall not be left unattended.
6. Fax machines and printers shall be kept in secure areas.
7. When faxing PPI, the recipients should be called in advance to ensure the fax is properly managed upon receipt.
8. When finished faxing, copying or printing all documents containing PPI should be removed from the machines promptly.

Database Integrity

The CHO must not intentionally cause corruption of the Homeless Resource Council of the Sierras' HMIS in any manner. Any unauthorized access or unauthorized modification to computer system information, or interference with normal system operations, will result in immediate suspension of HMIS licenses held by the CHO, and suspension of continued access to the Homeless Resource Council of the Sierras' HMIS by the CHO.

The HMIS Lead will investigate all potential violations of any security protocols. Any user found to be in violation of security protocols will be subject to sanctions, as described in the HMIS Policies and Procedures Manual. Individual users may be subject to disciplinary action by the employer CHO.

Disaster Recovery

Homeless Resource Council of the Sierras' HMIS data is stored by Bowman Systems, LLC in secure and protected off-site locations with duplicate back-up. In the event of disaster, the HMIS System Administrator will coordinate with Bowman Systems, LLC to ensure the HMIS is functional and that data is restored. The HMIS Lead Agency will communicate to CHOs when data becomes accessible following a disaster.

Contracts and other arrangements

The HMIS Lead shall retain copies of all contracts and agreements executed as part of the administration and management of the HMIS or required to comply with HUD requirements for a minimum of seven-years.

Homeless Resource Council of the Sierras' HMIS
PRIVACY PLAN

Data Collection Notice

Agencies that contribute HMIS data must let clients know that personal identifying information is being collected, and the reasons for taking this information. To meet this requirement, agencies may post the following language in places where intake takes place:

> We collect personal information directly from you for reasons that are discussed in our privacy notice. We may be required to collect some personal information by law or by organizations that give us money to operate this program. Other personal information that we collect is important to run our programs, to improve services for homeless persons, and to better understand the needs of homeless persons. We only collect information that we consider to be appropriate.

Agencies must obtain consent from clients using the Homeless Resource Council of the Sierras' HMIS Client Release of Information form.

Privacy Notice

Each agency is required to publish and post on its web site a Privacy Notice describing its policies and practices for use of protected personal information, and must provide a copy of its Privacy Notice to any individual upon request. The agency must post a sign stating the availability of its Privacy Notice to any individual who requests a copy.

Accountability

Agencies must require staff to sign an agreement that acknowledges receipt of a copy of the Privacy Notice and that pledges to comply with the Privacy Notice. The Homeless Resource Council of the Sierras' HMIS User agreement contains this language and enables each CHO to meet this requirement.

A CHO must establish a written policy for accepting and considering questions or complaints about its privacy and security policies and practices.

Access and Correction

In general, agencies must allow an individual to inspect and to have a copy of any information about the individual, and must offer to explain any information that the individual may not understand. Agencies must consider any request by an individual for correction of inaccurate or incomplete information about the individual, but is not required to remove any information. However, the agency may mark information as inaccurate or incomplete and may supplement it with additional information.

The agency may deny access to personal information for any of the following reasons, and should describe possible reasons in its Privacy Notice:

1. Information compiled in reasonable anticipation of litigation;
2. Information about another individual;
3. Information obtained under a promise of confidentiality if disclosure would reveal the source of the information; or

4. Information, the disclosure of which would be reasonably likely to endanger the life or physical safety of any individual.

The agency can reject repeated or harassing requests for access or correction. An agency that denies an individual’s request for access or correction must explain the reason for the denial to the individual and must include documentation of the request and the reason for the denial as part of the protected personal information about the individual.

Purpose and Use Limitations

Agencies may use or disclose personal identifying information from HMIS under the following circumstances: (1) To provide or coordinate services to an individual; (2) for functions related to payment or reimbursement for services; (3) to carry out administrative functions, including but not limited to legal, audit, personnel, oversight and management functions; or (4) for creating de-identified personal identifying information.

Certain disclosures may be required due to provider obligations that go beyond the privacy interests of clients. The following additional uses and disclosures are recognized by HUD, and the Springfield Office of Housing may provide additional guidance regarding these circumstances (each of which is described in more detail in the HUD 2004 HMIS Technical Standards):

1. Uses and disclosures required by law
2. Uses and disclosures to avert a serious threat to health or safety
3. Uses and disclosures about victims of abuse, neglect or domestic violence
4. Uses and disclosures for academic research purposes
5. Disclosures for law enforcement purposes

Confidentiality

Each agency must develop and implement written procedures to ensure: (1) All records containing protected identifying information of any individual or family who applies for and/or receives Continuum of Care assistance will be kept secure and confidential; (2) The address or location of any family violence project assisted with Continuum of Care funds will not be made public, except with written authorization of the person responsible for the operation of the project; and (3) The address or location of any housing of a program participant will not be made public, except as provided under a preexisting privacy policy of the recipient or subrecipient and consistent with State and local laws regarding privacy and obligations of confidentiality.

Protections for victims of domestic violence, dating violence, sexual assault, and stalking

Victim service providers are prohibited from entering data into HMIS. Other agencies must be particularly aware of the need for confidentiality regarding information about persons who are victims of domestic violence, dating violence, sexual assault, and stalking. Additional protections for these clients includes explicit training for staff handling personal identifying information of the potentially dangerous circumstances that may be created by improper release of this information.

Other Requirements

All agencies that contribute HMIS data must comply with the baseline privacy requirements described in this Privacy Plan. A CHO must comply with federal, state and local laws that require additional confidentiality protections. When a privacy or security standard conflicts with other Federal, state, and local laws to which the CHO must adhere, the CHO must contact the HMIS Lead Agency and collaboratively update the applicable policies for the CHO to accurately reflect the additional protections.

Homeless Resource Council of the Sierras HMIS

Data Collection Notice

We collect personal information directly from you for reasons that are discussed in our privacy statement.

We may be required to collect some personal information by law or by organizations that give us money to operate this program. Other personal information that we collect is important to run our programs, to improve services for homeless persons, and to better understand the needs of homeless persons.

We only collect information that we consider to be appropriate.

Homeless Resource Council of the Sierras' HMIS

DATA QUALITY PLAN

Data Quality Benchmarks and Controls

The chart below identifies the standards that the CoC will monitor as part of its data quality plan, as well as the monitoring procedures for each standard. The Coverage standard applies to the CoC as a whole. All other standards apply to CHOs and programs.

General Principle	Specific Principle	Expected Benchmark	Monitoring Procedure Who? How often?
Coverage	All lodging and non-lodging homeless programs in the CoC report HMIS data	95% Emergency shelter beds, Outreach, and SSVF report into HMIS. 100% Rapid Rehousing and Homelessness Prevention beds report into HMIS. 75% Permanent supportive housing and transitional housing beds report into HMIS.	HIC provides annual report. HMIS Lead will report status quarterly to Board of Directors.
Completeness	All clients entered	95% of clients must have all universal data entered. 95% of clients qualifying for Interim/Update assessment must have assessment completed.	Monthly reports sent to participating agencies.
	Complete exit data entered	No more than 5% missing exit assessments. No more than 5% incomplete exits assessments (includes completion of exit assessment)	Check missing exit assessments on monthly missing data report. The HMIS Administrator will spot check two (2) sites every month, checking recent exit assessments for completeness.
Accuracy	Accurate data entered by staff	At least 80% of the records must be entered accurately	Annual visit to conduct random spot check of paper files against HMIS. Pull lesser of 10% or six (6) records and look for client data in the database.

	Changing data kept up to date	Active clients with data elements that have changed should be updated within 30 days.	The Homeless Resource Council of the Sierras HMIS Staff will review with the CHO Site Manager in bi-annual visits.
Timeliness	Data are entered soon after collected	Clients of all project types must be entered within one (1) week of intake.	Monthly reports to agencies.
Consistency	Common interpretation of questions and answers	Data will be reviewed at the quarterly HMIS Committee meetings.	The HMIS Administrator will compare aggregate data by users for same population to look for unusual patterns on a quarterly basis. Inconsistencies found during the month will be noted and discussed at the quarterly HMIS Committee meeting.
	Common knowledge of what fields to answer	95% of required fields completed	Monthly check of required fields in system – 95% of records have complete minimal fields.

Roles and Responsibilities

HRCS Board of Directors

The Board of Directors is responsible for oversight of data quality, and will review high-level data quality reports quarterly. The Board will act upon recommendations made by the HMIS Committee and the HMIS Lead.

HMIS Committee

The HMIS Committee is responsible for ongoing oversight of progress toward the CoC's meeting of all Data Quality Benchmarks system-wide. It will regularly review data quality reports, assist agencies in gaining compliance, and ensure that required reports and trainings are made available for the agencies. It will provide quarterly updates to the CoC Board of Directors on progress of the data quality plan and provide regular reports on the quality of the CoC's data.

HMIS Lead Agency

The HMIS Lead is responsible for monitoring CHOs to ensure that the standards on the extent and quality of data entered into the Homeless Resource Council of the Sierras' HMIS set forth in these policies and procedures are met to the greatest possible extent and that data quality issues are quickly identified and resolved.

The HMIS Lead will run data quality reports and will directly provide agencies with the reports for their projects via email. The regularity of the reporting provides participating agencies with the opportunity to review data and update any missing elements before the HMIS Administrator assesses progress. Monthly reports include the following:

1. ***Missing Data – Assessments***: This report alerts participating agencies if they have failed to record detailed assessment information. It identifies where they have entered a new participant into the database, but have failed to provide required assessments.
2. ***Missing HUD Universal Data Elements***: The HMIS Administrator will track completion of universal data elements on a monthly basis.

The HMIS Lead Agency will monitor at least annually the projects that are funded by the CoC. It will review data quality reports, bed utilization reports, and compliancy with the Data Quality Plan. It will report and make recommendations to the CoC Application Committee on the quality and usability of data submitted by CoC-funded agencies.

Contributing HMIS Organizations

CHOs are responsible for training and monitoring HMIS users to ensure understanding of and compliance with data quality standards.

Each CHO is responsible for addressing any issues identified through the data quality monitoring. Where data errors are identified, the CHO must correct the errors within 30 days. Where overall systemic data quality issues are identified, the CHO must participate with the HMIS Lead in creation of a corrective action plan.

Remedial Actions

The goal of data quality monitoring is for the CoC to obtain and maintain high-quality data. In order to meet this goal, CHOs with repeated data quality issues will be initially provided with increasing levels of support to assist in resolving data issues. Support may include additional training and/or technical assistance from the HMIS Lead, Bowman Systems, LLC, or a qualified consultant.

The CHO may be required to submit a corrective action plan to the HMIS Lead, and to provide regular reports to the HMIS Lead on progress toward implementing the identified corrective actions. Components of a corrective action plan may include:

- Developing and following a schedule of actions for carrying out HMIS-related tasks, including schedules, timetables, and milestones;
- Establishing and following an HMIS data quality plan that assigns responsibilities for carrying out remedial actions; and
- Increased monitoring and reporting of HMIS data quality.

If increased support does not result in the CHO meeting data quality standards, the CHO may be subject to sanctions, as described in the Homeless Resource Council of the Sierras' HMIS Policies and Procedures Manual.