A Tradition of Stewardship
A Commitment to Service

Napa County Continuum of Care

Homeless Management Information System (HMIS)

Policies & Procedures Manual

May 2023

Table of Contents

HMIS CONTACT INFORMATION

HMIS Lead Agency
Napa County
Housing and Homelessness Services

Karina Gallegos-Ruiz
HMIS System Administrator
Napa County
Housing and Homelessness Services
Karina.Gallegos-Ruiz@countyofnapa.org

HMIS Technical Support
Bitfocus Inc.
Napa@Bitfocus.com

INTRODUCTION

The United States Department of Housing and Urban Development (HUD) defines the Homeless Management Information System (HMIS) as the information system designated by the Continuum of Care (CoC) to comply with HUD's data collection, management, and reporting standards. HMIS collects data to measure the efficacy of services provided to homeless persons and those persons at risk of homelessness. It is intended to generate unduplicated counts of homeless persons, as well as explore the nature of homelessness in general. The data collected by HMIS are used to drive evidence-based decisions at the local, state, and national level, with the ultimate goal to eradicate homelessness in the United States.

This manual outlines the policies, procedures, guidelines, and standards for Napa CoC HMIS operations. It contains the HMIS operating procedures and its privacy, security, and data quality plans. The manual is designed to be used in tandem with the Napa CoC HMIS Governance Charter, which provides a structure for decision-making and formalizes the roles and responsibilities of all HMIS entities.

HMIS and its policies and procedures are structured to comply with the standards set for HMIS as described in the 2004 HMIS Data and Technical Standards Final Notice, FY2022 HMIS Data Standards Manual, and additional HUD guidance. The HMIS Lead Agency, HMIS System Administrator, Partner Agencies, Agency Administrators, Designated Security Officers, and End Users are all responsible for maintaining compliance with the HMIS Policies & Procedures and all federal, state, and local laws and regulations.

If you have any questions about the HMIS Policies & Procedures, please contact the HMIS System Administrator.

DEFINITIONS

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

Continuum of Care- a regional or local planning body that coordinates housing and services funding for homeless families and individuals

End User- Partner Agency staff responsible for entering client level data in HMIS

HMIS Lead Agency - The entity designated by the Napa CoC to oversee the day-to-day administration of the HMIS system

HMIS System Administrator– HMIS Lead Agency staff responsible for oversight the day-to-day administration of the HMIS system

Homeless Management Information System - local information technology system used to collect client-level data and data on the provision of housing and services to homeless individuals and families and persons at risk of homelessness.

Partner Agency- Any agency that makes reasonable efforts to record all HUD-defined Universal Data Elements and all other required data elements as outlined by HUD funding requirements on all clients served, and discloses these data elements to the HMIS Lead Agency

Personally Protected Information- Any information about a homeless living client or homeless individual that; Identifies, either directly or indirectly, a specific individual; can be manipulated by a reasonably foreseeable method to identify a specific individual; or can be linked with other available information to identify a specific individual

Program- the source of funding that the organization is receiving to run its project (e.g. CoC Program funding for ABC Transitional Housing project)

User- individual with access to the system for data entry, editing of client records, viewing of client records, report writing, administration or other essential activity associated with carrying out Partner Agency responsibilities.

OPERATIONS

HMIS Participation Policy

Mandated Participation

All agencies with programs funded to provide homeless services by Napa County, Bureau of Homeless and Housing Services (BHHS) and/or HUD and/or State of California must meet the minimum HMIS participation standards as defined in the HMIS Participation Policy.

Voluntary Participation

Although Partner Agencies are only required to meet minimum participation standards for programs with mandated participation, The HMIS Lead Agency and the CoC strongly encourage Partner Agencies to fully participate with all their homeless programs.

While the CoC cannot require non-CoC funded agencies to participate in HMIS, the CoC works strongly with such agencies articulate the benefits of HMIS and to strongly encourage their participation in order to achieve a comprehensive and accurate understanding of homelessness in Napa County.

Minimum Participation Standards

Partner Agencies must:

1. Collect all universal data elements, as defined by HUD, for all clients served by all programs funded through the state of California, HUD or Napa County;
2. For all such programs, enter federally required and county required client-level data into HMIS;
3. Comply with all Napa County HMIS Policies & Procedures; and
4. Comply with all HUD regulations for HMIS participation.

Agency Participation Requirements

Designation of Agency Administrator

Partner Agencies must designate at least one Agency Administrator who is the agency's point person and specialist regarding HMIS. The Agency Administrator is responsible for:

- Provide a single point of communication between HMIS users and the HMIS Lead Agency regarding HMIS issues;
- Ensure the stability of the Agency connection of HMIS to the Internet;
- Manage HMIS End User licenses/staff according to HMIS Napa County CoC Policies and Procedures;
- Configure Program descriptors and Provider Preferences in HMIS (Assessment, Referrals, Services, and other applicable configurations);
- Provide support for generating Agency reports;
- Oversee resolution of data-quality issues (e.g., ensuring universal data elements are entered in HMIS for all clients); and
- Monitor compliance with standards of client confidentiality, data collection and entry, entry, and data retrieval.

Provision of Hardware and Connectivity

Partner agencies must ensure end users have access to workstations that meet the minimum specification for Clarity:

- **Computer and/or Mobile Platform**
  - PC or Mac. Clarity Human Services is also designed to be a fully mobile platform. Users on mobile devices such as Apple iOS (iPhone, iPad), Google Android, or Windows Phone gain additional functionality through GPS and

camera hardware, and a fully optimized touch interface for a native user experience on these devices.

- **Monitor**
  - Screen Display - 1600 x 1200 (XGA) recommended
- **Processor**
  - A Dual-Core processor is recommended.
- **Internet Connection**
  - Broadband Internet is required for each workstation accessing HMIS. To optimize performance, all agencies are encouraged to secure a high-speed Internet connection with a cable modem, DSL, or T1 line.
- **Browser**
  - Accessible from any modern web browser, including the following: Firefox, Chrome, and Safari.

HMIS Implementation

Agency Implementation

Prior to setting up a new Partner Agency within HMIS database, the HMIS System Administrator shall:

1. Request and receive approval from the CoC to set up a new Agency;
2. Execute an HMIS Participation Agreement with the Partner Agency;
3. Complete Annual HMIS Security Checklist
4. The New Partner Agency will review the following:
   a. Napa County Continuum of Care Homeless Management Information System Governance Charter
   b. Napa County Continuum of Care HMIS Policies and Procedures Manual
   c. Naoa County Required HMIS Data Elements
   d. Napa County Continuum of Care Governance Charter
5. In conjunction with Lead Agency Security Officer, ensure the Partner Agency has appropriate policies and procedures in place to comply with the Security Plan and Privacy Plan;
6. Work with the Agency Administrator to input applicable program specific data elements into the HMIS; and
7. Work with the HMIS Lead Agency to migrate legacy data, if applicable, and within the scope of normal HMIS functions. Data migration needing additional HMIS or third-party vendor intervention will be addressed on a case-by-case basis.

User Implementation

Eligible Users

Each Partner Agency will request HMIS access only for staff who are actively engaged in data entry, editing of client records, viewing of client records, report writing, administration or other essential activity associated with carrying out Partner Agency responsibilities. The HMIS

Lead Agency will authorize use only to those who meet these requirements. The HMIS Lead Agency may request additional information regarding a new user's need for HMIS access to verify need for access. The HMIS Lead Agency reserves the right to review and terminate licenses for users who have not accessed HMIS in over 60 days.

The HMIS Lead Agency will fund one lead agency license and one end user license for all agencies participating in HMIS as of May 30, 2023. Additional licenses will be billed in accordance with the HMIS Lead Agency fee structure and will be billed the following month after activation. Any agency mandated to participate in HMIS by AB977 that was *not* participating in Napa's HMIS as of April 1, 2023, will be required to purchase all licenses.

Any agency mandated to participate in HMIS by AB977 that was not participating in Napa's HMIS as of May 30, 2023, will be required to purchase all licenses.

User Requirements

All users must complete the following requirements prior to being authorized access to the HMIS:

1. Complete all initial training required by the HMIS System Administrator and Agency Administrator to include;
    a. User Policy, Responsibility Statement & Code of Ethics
    b. Watch Protecting Data in an HMIS Environment: Privacy, Security and Confidentiality (45 Min.)
    c. Watch Clarity Human Services: General Training from Bitfocus (75 Min.)
2. Complete an agency sponsored background check as described in the HMIS Security Plan;

User Responsibilities

Users are accountable for their actions, and for any actions undertaken with their username and password. All users are responsible for awareness of and compliance with all HMIS policies and procedures, including operating procedures and the security, privacy, and data quality plans.

New User Set Up

If the Partner Agency wants to request system use for a new user, the agency's Executive Director, Agency Administrator or authorized designee must

1. Determine the access level of the proposed HMIS user; and
2. Submit a New Staff Access Request Form.

The HMIS System Administrator will verify that all user requirements have been completed prior to authorizing system access with the assistance of Bitfocus

HMIS Technical Support

As unanticipated technical support questions on the use of the HMIS application arise, end users will follow these procedures to resolve those questions:

During the normal Napa County HMIS business hours:

1. Begin with utilization of the on-line help and/or training materials at http://help.clarityhs.com/;
2. If the question is still unresolved, direct the question to the HMIS System Administrator; and
3. If the question is still unresolved, the HMIS System Administrator will direct the question to the Bitfocus, Inc. team by opening a Ticket system.

After the normal Napa County HMIS business hours:

1. Begin with utilization of the on-line help and/or training materials at http://help.clarityhs.com/;
2. If the question is still unresolved and can wait to be addressed during the following business day, wait and follow the normal business hours procedure outlined above; or
3. If the question cannot wait, direct the technical support question to http://help.clarityhs.com/ or send an email to support@bitfocus.com or call (702) 614-6690 ext. 2.

There are times that Clarity is unavailable because Bitfocus Systems is performing necessary backup and maintenance of the HMIS database. These are usually in the late evenings when as few people as possible need access to the system. When the HMIS Lead Agency receives notice of a planned interruption of service for other reasons or for an abnormal amount of time, the HMIS Lead Agency will notify Agency Administrators and End Users via email. If there is an unplanned interruption to service, the HMIS System Administrator will communicate with Clarity, and Agency Administrators and End Users will be notified of any information regarding the interruption as it is made available.

DATA PRIVACY PLAN

Overview

The 2004 HMIS Technical and Data Standards require the implementation of a HMIS data privacy plan to protect Protected Personal Information (PPI) while allowing for reasonable, responsible and limited uses and disclosures of data. This privacy plan addresses how client data is collected, stored, and used. It is intended to ensure that a client whose information is being used and disclosed by a Partner agency is informed and has choice in how their information is used.

Client Notification and Consent

Partner Agencies are responsible for ensuring that all clients are notified of the purpose of data collection, how their data may be used or disclosed, and ensuring appropriate client consent is obtained for uses and disclosures. Partner agencies are required to use the forms specified in this section, which are available at http://countyofnapa.org/HHSA/HomelessServices/HMIS.

Each Partner Agency must provide reasonable accommodations to persons with disabilities and to persons with limited English proficiency to ensure their understanding of the HMIS Privacy Posting, Privacy Notice, and/or Release of Information.

Public Statement

Partner Agencies must post the Napa County HMIS and Confidentiality Posting at each intake or comparable location. This posting advises clients of the reasons for data collection. Agencies must also post the posting on the agency website, if applicable.

Privacy Notice

Each client must be provided a copy of the Napa County Continuum of Care HMIS Privacy Notice ("HMIS Privacy Notice"). This notice advises clients of the purpose and use limitations of their PPI. Partner Agencies must offer to review the Privacy Notice with the client. Clients receiving services virtually should be offered a verbal review of the HMIS Privacy Notice and provided a written copy of the HMIS Privacy Notice via mail or other means or at the first in-person contact, depending on client preference.

Written Consent/ Release of Information

Client information cannot be shared in HMIS until the client has provided consent. If a client declines to provide written or verbal consent for information to be shared between partner agencies, their data must be entered into HMIS, but made private or deidentified. Clients cannot be refused service for declining to provide written consent.

Consent to share information is documented using the Napa County Continuum of Care HMIS Client Informed Consent and Release of Information ("ROI") form. It is the responsibility of each Partner Agency to verify that a current ROI is uploaded to the client record prior to entering PPI into HMIS. If a current ROI is not on record, the Partner Agency must complete a ROI with the client prior to entering PPI into HMIS.

The ROI must be signed and dated by the client whenever a client is seen in person. In the case that a client is receiving services virtually, the Partner Agency will provide a verbal explanation of the ROI and seek verbal consent. Agency Staff will complete, sign and date the release of information, noting “Virtual Services- Verbal Consent Provided” in the signature space. Partner Agency Staff will offer to mail or otherwise provide a copy of the ROI to the client. When verbal consent is used, a ROI must be signed by the client at the first face to face interaction.

Completed forms must be uploaded to HMIS upon completion. All ROI forms must be retained in the agency’s client case management file for record keeping and auditing purposes in accordance with agency policies and procedures.

Revocation of Consent

The current ROI form does not have an expiration date and does not expire. ROI form revisions prior to March 2021 may list an expiration date and expire on that date. Client consent remains valid until revoked. Client can revoke consent at any time. Clients must notify the Partner Agency in writing of their revocation of consent. Revocation of consent will not be retroactive. Written requests to revoke consent must be uploaded to HMIS and retained in the agency’s client case management file.

Data Collection Limitations

Each agency shall only solicit or input into HMIS client information that is essential to providing services to the client.

The Health Insurance Portability and Accountability Act (HIPAA), the Violence Against Women Act (VAWA), the Family Violence Prevention and Services Act (FVPSA), 42 CFR Part 2., and other Federal, State and local laws may require certain privacy safeguards, and/or client consent to collect and retain personally protected information (PPI). It is the responsibility of the Partner Agency to be aware of and comply with all federal data privacy or security laws that may apply to a program. Partner Agency must comply with the requirements that ensure the greatest protection for the client’s PPI.

Data Purpose and Use Limitations

Uses are internal activities for which users interact with participant PPI. Disclosures of PPI occur when users share PPI with an external entity.

PPI may be used or disclosed for the following purposes:

- For functions related to payment or reimbursement for services
- To carry out administrative functions, including but not limited to legal, audit, personnel, oversight, and management functions
- For creating de-identified data from PPI
- Uses and disclosures required by law
- Uses and disclosures to avert a serious threat to health or safety

- Uses and disclosures about victims of abuse, neglect, or domestic violence
- Uses and disclosures for research purposes
- Uses and disclosures for law enforcement purposes
- Participants' access to their own information
- Disclosures for oversight of compliance with HMIS data privacy and security standards

Access & Correction Standards

The client has the right to view and request corrections on their own data. The Partner Agency must offer to explain information that the client does not understand. The Partner Agency must consider any request by the client to correct inaccurate or incomplete PPI, by removing, supplementing, or simply marking the information inaccurate or incomplete.

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

If a Partner Agency is a Victim Service Provider (as defined by the HEARTH Act), it cannot disclose a participant's PPI in HMIS. It is the responsibility of the Partner Agency to determine if they are designated as a Victim Service Provider. Such providers must use a relational database comparable to HMIS in its capacity to support HUD data privacy and security requirements and, at a minimum, meet Data Standards requirements and produce HUD-required reporting files.

Aggregate Data Use

HMIS client data will be released only in aggregate, for any purpose beyond those specified in the Privacy Plan. All released data must be anonymous, either by removal of all identifiers and/or all information that could be used to infer an individual or household identity.

Training

Each Partner Agency is responsible for developing a process for regular training all agency staff on the HMIS Privacy Plan and all internal privacy policies and procedures. Each Partner Agency must ensure that all staff are trained on the HMIS Privacy Notice, receive a copy of the privacy notice, and sign acknowledging receipt of the HMIS Privacy Notice.

The HMIS System Administrator will provide initial and annual training to all Users on the HMIS Privacy Plan.

Monitoring

All Partner Agencies are responsible for developing internal policies and procedures to regularly audit compliance with privacy practices, and accept and investigate questions or complaints about its privacy practices.

The HMIS System Administrator is responsible for ensuring that each agency has appropriate policies and procedures in place to ensure compliance with the privacy plan. The HMIS System Administrator will review Partner Agency policies and procedures prior to approving the agency for HMIS implementation. The HMIS Lead Agency will investigate any client complaint filed directly with the HMIS Lead Agency in conjunction with the Partner Agency.

Enforcement

Partner Agencies are responsible for developing internal process that establish sanctions for staff non-compliance with agency privacy practices.

DATA SECURITY PLAN

Overview

Data security is the protection of PPI from unauthorized access, disclosure, use, or modification. This security plan is intended to ensure the confidentiality, integrity, and availability of all HMIS information; protect against reasonably anticipated threats or hazards to security; and ensure compliance by end users.

Responsibilities

Partner agencies are responsible for developing agency policies and procedures to ensure compliance with the data security plan.

The HMIS Lead Agency is responsible for monitoring Partner agency compliance and enforcing sanctions for non-compliance with the data security plan.

Administrative Security

Security Officer Designation

The HMIS Lead Agency and each Partner Agency must designate a Security Officer to be responsible for ensuring compliance with applicable security standards.

Lead Security Officer

The Lead Security Officer may be an HMIS System Administrator, or another employee, volunteer or contractor designated by the HMIS Lead Agency who has completed HMIS Privacy and Security training and is adequately skilled to assess HMIS security compliance.

The Lead Security Officer is responsible for:

- Assessing the security measures in place prior to establishing access to HMIS for a new Partner Agency,

- Ensuring that hardware, software, and physical environments that store, transmit, or process HMIS data are compliant with the security plan;
- Ensuring that all users complete security training prior to being given access to HMIS and annually thereafter;
- Responding to all substantiated violations of any security protocols; and
- Reviewing and maintaining a file of Partner Agency annual compliance certification checklists, and conducting an annual security review of all Partner Agencies.

Partner Agency Security Officer

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

The Partner Agency Security Officer is responsible for:

- Conducting an initial and annual security review for any workstation that will be used for HMIS purposes;
- Continually ensuring each workstation within the Partner Agency used for HMIS data collection or entry meets the standards in the security plan;
- Implementing agency policies procedures to ensure and monitor its compliance with the security plan, including enforcement of sanctions for noncompliance;
- Ensuring that end users complete annual security training;
- Establishing a procedure for accepting and investigating questions, complaints, or suspected breaches of security practices; and
- Completing the annual security review and Annual HMIS Security Checklist, and forwarding the Checklist to the Lead Security Officer.

Background Checks

Each Partner Agency must complete a background check on the Agency Security Officer and all Users. The HMIS Lead Agency must complete a background check on the HMIS System Administrator and Lead Security Officer. The Lead Agency and Partner Agencies must retain the results of all background checks in the employee’s personnel file.

No prospective user will be given a HMIS access if he or she has entered a plea of nolo contendere (no contest) or has been found guilty of any fraud (including identity theft) or stalking related felony crimes punishable by imprisonment of one year or more in any state. Crimes considered in the category of fraud or identity theft include bank fraud, blackmail, bribery, computer fraud, credit card fraud, extortion, forgery, health care fraud, larceny/theft, money laundering, telemarking fraud, and welfare fraud.

The background check must include local and state records; agencies are strongly encouraged to include federal records as well. A background check may be conducted only once for each person unless otherwise required by HUD or agency policy. The results of the background check must be retained in the employee's personnel file.

Workstation Security

Accessing HMIS from a Laptop or Desktop

- If a workstation is in a public area, it must always be staffed by a User.
- Workstations in use in public areas must be arranged so that unauthorized users cannot view the screen when it is in use.
- HMIS Users must log out of HMIS when not actively using HMIS.
- Workstations must automatically turn on a password protected screen saver when the workstation is temporarily not in use.
- When workstations are not in use and staff are not present, the workstation must be stored and secured to prevent unauthorized access or theft.
- Access to HMIS will be allowed only from devices specifically identified by the Partner Agency's Executive Director or authorized designee and Partner Agency Security Officer.
- The owner, authorized user, model, and serial number of each workstation that is used to access HMIS must be written down and on file with the Agency Security Officer before the device is used to access HMIS.

Accessing HMIS from a Phone or Tablet

End Users accessing HMIS from a mobile device, such as a phone or tablet must follow the policy for accessing HMIS from a laptop or desktop workstations, in addition to the following:

- Mobile devices that are used to access HMIS must not store or "memorize" HMIS-related passwords; End Users should be required to re-enter their password each time they log on.
- Whenever possible, mobile devices that are used to access HMIS should be registered for remote detection and remote wiping, so that a lost or stolen device can be located and/or reset to factory settings.
- No End User may register more than one mobile device at a time for HMIS access. Each such device must be configured to lock its screen after no more than 60 seconds of inactivity and protected with a unique, robust password.

- The owner, authorized user, model, and serial number of each mobile device that is used to access HMIS must be written down and on file with an Agency's Security Officer before the device is used to access HMIS.

User Authentication

User Accounts

The HMIS System Administrator is responsible for managing user accounts for all Partner Agencies in accordance with the User Implementation policy. The assigned user type will determine each user's individual access level to data, and HMIS System Administrator must regularly review user access privileges.

Rescinding User Access

The Partner Agency Administrator is responsible for informing the HMIS System Administrator within 24 hours of any user that has left the agency or otherwise does not meet the End User requirements to access HMIS. The HMIS System Administrator is responsible for removing the user from the system within 24 hours.

User Passwords

Each user will be assigned a unique identification code (User ID), preferably the first initial and last name of the user.

A temporary password will be automatically generated by the HMIS System Administrator when a new user is created. The HMIS System Administrator will communicate the password to the user. The user will be required to establish a new password upon their initial login. This password will need to be changed every 90 days. A password cannot be used again until another password has expired. Passwords must be between 8 and 16 characters long, contain at least two numbers and one special character, and should not be easily guessed or found in a dictionary. The password format is alphanumeric and is case-sensitive.

Users are prohibited from sharing passwords, even with supervisors. Usernames and passwords cannot be stored or displayed in any publicly accessible location.

Password Reset

Except when prompted by Clarity to change an expired password, users cannot reset their own password. The HMIS System Administrator will request assistance from Bitfocus to temporarily reset a password.

Unsuccessful Login

If a user unsuccessfully attempts to log in 3 times, the User ID will be “locked out”, their access permission will be revoked, and they will be unable to regain access until their User ID is reactivated by the HMIS System Administrator with the assistance of Bitfocus.

Virus Protection

Each workstation must have anti-virus and anti-spyware programs in use and properly maintained with automatic installation of all critical software updates. Good examples of anti-virus software include McAfee and Symantec (Norton) Security systems, among others.

Firewalls

All workstations accessing HMIS need to be protected by a firewall. If the workstations are part of an agency computer network, the firewall may be installed at a point between the network and the internet or other systems rather than at each workstation.

Copy Security

Hard Copy Security

- Documents printed from HMIS containing PPI must be sent only to printers in secure locations and promptly collected.
- Hard copies must be securely stored in an area that is not publicly accessible when not in use.
- Hard copies containing PPI must always be supervised when in use.
- The printed materials must be destroyed (e.g., shredded) as soon as they are no longer needed, and the printer must be checked at least once daily to identify and dispose of any unclaimed documents.

Electronic Copy Security

An electronic copy refers to data copied from HMIS and stored in another electronic medium, such as a PDF file or “screenshot”.

- Users may only store HMIS data containing PPI on devices approved by their agency.
- Users may not store HMIS data containing PPI on hard drives or removable media that can be accessed by non-system users.
- Users are responsible for safeguarding HMIS PPI that users store on agency-owned devices.

- Electronic transmission of HMIS data containing PPI will be limited to secure direct connections or, if transmitted over the internet, the data is sent via encrypted email or password protected file.
- Email communications including HMIS data cannot include client names. The HMIS Unique Identifier should be used in place of the client name.
- Partner Agencies are responsible for developing additional policies and procedures for protecting electronic data from theft, loss, or unauthorized access.
- Before disposing of hard drives, USB drives, or other portable electronic media used to store PPI, the Partner Agency will consult with their agency HMIS Security Officer.

System Security

Data Transmission and Storage

Bitfocus stores and transmits data using multiple technical controls that meet or exceed the requirements put forth by HUD, including 2048 bit SSL encryption. Bitfocus Systems is contractually obligated to provide data storage in a facility that provides 24/7 physical and electronic security and monitoring.

Disaster Recovery Plan

Bitfocus Systems maintains a daily backup of HMIS data. Backup data is stored by Bitfocus in a secured facility for one year. After one year, the backup data is fully destroyed.

In the case of a disaster, the HMIS Lead Agency will notify Bitfocus that that data must be recovered and restored. The HMIS Lead Agency will notify all Partner Agencies and the CoC promptly via email that recovery and restoration is in process. Bitfocus will provide data recovery and restoration within one day.

Training

- The Lead Security Officer will provide initial and annual training to all users on the security plan.
- Partner Agency Security Officers are responsible for providing initial and annual training to users on agency level security policies and procedures.

Monitoring

The Partner Agency Security Officer must complete an annual security review and document the reviewing using the Annual HMIS Security Checklist to ensure compliance with the security plan. The Partner Agency must submit a copy of the review to the Lead Security Officer. The Lead Agency Security Guard will review and approve the submission and retain copies of all submitted Annual HMIS Security Checklists.

Incident Response and Policy Enforcement

The security plan is intended to prevent, to the greatest degree possible, any security incidents. However, should a security incident occur, the following procedures should be followed.

1. Any user who becomes aware of or suspects a breach of HMIS system security and/or client privacy must immediately report that breach to the Partner Agency Security Officer.
2. In the event of a breach resulting from suspected or demonstrated noncompliance by an end user, the Partner Agency Administrator should request the HMIS System Administrator deactivate the end user's User ID until an internal agency investigation has been completed.
3. Following an internal investigation, the Partner Agency Security Officer shall notify the Lead Security Officer of any substantiated incidents that may have resulted in a breach of HMIS system security and/or client privacy (whether a breach is definitively known to have occurred). If the breach resulted from suspected or demonstrated noncompliance by an end user, the HMIS Lead Agency reserves the right to deactivate the User ID for the end user in question pending further investigation.
4. Within 1 business day after the Lead Security Officer receives notice of the breach, the Partner Agency Security Officer and Lead Security Officer, will jointly establish an action plan to analyze the source of the breach and actively prevent future breaches. The Lead Agency Security Officer will be responsible for consultation with BitFocus if indicated. The action plan shall be implemented as soon as possible, and the total term of the plan must not exceed 30-days.
5. If the Partner Agency is not able to meet the terms of the action plan within the time allotted, the HMIS Lead Agency may elect to terminate the Partner agency's access to HMIS. The partner agency may appeal to the appropriate body of the Continuum of Care for reinstatement to HMIS following completion of the requirements of the action plan.
6. In the event of a substantiated breach of client privacy through a release of PPI in noncompliance with the provisions of HMIS policies and procedures, the Partner Agency will attempt to notify any impacted individual(s).
7. The Lead Security Officer will notify the appropriate body of the Continuum of Care of any substantiated release of PPI in noncompliance with the HMIS policies and procedures.
8. The HMIS Lead Agency will maintain a record of all substantiated releases of PPI in noncompliance with the HMIS Policies and Procedures for 7 years.
9. The Continuum of Care reserves the right to permanently revoke a Partner Agency's access to HMIS for a breach of security or privacy.

DATA QUALITY PLAN

Overview

Data Quality refers to the reliability and validity of client-level data collected in HMIS. It is measured by the extent to which the data in the system reflects information in the real world. High quality data is vitally important to the success of the Napa CoC and Partner agencies, and critical to the work of ending homelessness in the Napa community. Good quality data allows for accurate assessment of outcomes and effective planning at the agency and community level. Poor quality data can negatively impact the ability of Partner agencies and the Napa community to receive funding for homeless services. This data quality plan is intended to ensure that HMIS data is timely, complete, and accurate.

Data Completeness

Universal Data Elements

Partner Agencies are responsible for ensuring that all HUD Universal Data Elements (UDEs) as defined by the HUD Data and Technical Standards, are collected and/or verified from all clients at their initial program enrollment or as soon as possible thereafter. The UDEs are included collectively on the Client Profile, Assessment, and HUD Entry and Exit assessments, which are on the Clarity Enrollment and Exit screens, respectively.

Partner Agencies must report client-level UDEs using the required response categories detailed in the "Data Types/Response Categories for Universal Data Elements" section of the HUD Data Standards Manual, located at https://www.hudexchange.info/resources/documents/HMIS-Data-Standards-Manual.pdf.

Program-Specific Data Elements

All Partner Agencies are responsible for ensuring that all Program-specific Data Elements, as defined by the HUD Data and Technical Standards, are collected from all clients that are served by applicable HUD-funded programs.

Partner Agencies must provide client-level data for the Program-specific Data Elements using the required response categories detailed in the "Required Response Categories" and Program-Specific Data Elements section of the HUD Data and Technical Standards.
The Program-specific Data Elements are located in the HUD Entry and Exit assessments, which are on the Clarity Enrollment and Exit screens, respectively.

Napa County Required Data Elements

In addition to the HUD required data elements, Napa County BHHS requires completion of all Napa County Required Data Elements, which are found in the Napa County Required Data Elements attachment, for all clients served in all programs.

Data Completeness Standard

All Partner Agencies will meet the following standard for data completeness:

- 100% of clients served will be entered into HMIS
- 95% of required data elements will be completed for all clients served

Data Timeliness

Partner Agencies will enter all required data elements in HMIS in a timely fashion.

Data Timeliness Standard

Program Type	**Timeframe**
Emergency Shelter	Less than 14 days from program entry
Non-Emergency Shelter	Less than 14 days from program entry
Shelter Plus Care	Less than 14 days from program entry
Transitional Housing Program	Less than 14 days from program entry
Permanent Supportive Housing	Less than 14 days from program entry
Other Rental Assistance Programs	Less than 14 days from program entry
Homeless Prevention & Rapid Rehousing	Less than 7 days from program entry
Outreach	Less than 45 days from initial contact

Data Accuracy

All End Users are responsible for entering accurate client data and correcting any inaccurate client data identified in a client record, including inaccurate data entered by a prior agency or program. The HUD HMIS Data Standards Manual, located at https://www.hudexchange.info/resources/documents/HMIS-Data-Standards-Manual.pdf , provides data collection instructions and descriptions of response fields for each data element. All End Users are responsible for ensuring that each data element is collected and recorded in accordance with the guidance provided in the current HMIS Data Standards Manual.

If duplicate records are identified, the Partner Agency Administrator will notify HMIS System Administrator via email within 3 days. The HMIS System Administrator will merge the records.

Data Accuracy Standard

All Partner Agencies will meet the following standard for data accuracy:

100% of data entered in HMIS will accurately reflect data collected in the agency file, information known about the client, and information reported by the client.

Training

Each End User must complete at least one session of training addressing data quality with the Lead Agency before being given HMIS login credentials. Reports training for interested users will be made available as needed. This training will include how to use existing canned reports.

Partner Agency Administrators are responsible for developing policies and procedures to ensure End Users receive ongoing training on data quality.

Monitoring

Partner Agency Administrators must develop policies and procedures monitoring of data accuracy, completeness, and timeliness on an at least quarterly basis. Partner Agencies that do not meet the data standards are responsible for developing and implementing a plan of correction.

The HMIS System Administrator will perform regular data integrity checks on the HMIS data, which will include the following steps:

- Run Annual Program Set Up Review, and a Quarterly Data Quality Report as determined by the HMIS Lead Agency and CoC HMIS Policy Committee;
- Notify Partner Agency of findings and timelines for correction;
- Re-run reports for errant agencies/programs, as requested. Follow up with Agency Administrators, if necessary;
- Notify Agency Executive Director if Agency Administrators are not responsive to required corrective actions; and
- Notify the CoC chair and the HMIS Lead Agency regarding any uncorrected data quality issues.

Enforcement

- Any patterns of error at a Partner Agency will be reported to the Agency Administrator through electronic mail.
- Partner Agencies are expected to correct data errors within thirty (30) days of notification.
- When patterns of error have been discovered, users will be required to correct their data entry techniques and will be monitored for compliance by the Lead Agency
- Programs under contract with the HMIS Lead Agency will be considered out of compliance with their HMIS Participation Agreement if they do not demonstrate a good faith effort to make necessary data corrections within (30) thirty days. This may place the program in default of the contract.
- If data is not up to date, Napa County will take the following steps:
    - A formal letter of notification to the CoC Chair and Agency Executive Director; and
    - Inclusion of the status of non-compliance of the organization in public reports.

ATTACHMENTS

1. **HMIS Agency Participation Agreement**
2. **HMIS Partner Agency System Administrator & Security Officer Designation**
3. **HMIS End User Agreement**
4. **HMIS New Staff Access Request Form**
5. **Napa County HMIS and Confidentiality Posting**
6. **HMIS Privacy Notice**
7. **Napa County Continuum of Care HMIS Client Informed Consent and Release of Information**
8. **Annual HMIS Security Checklist**
9. **Napa County Required HMIS Data Elements**
10. **Napa Continuum of Care HMIS Governance Charter**