HMIS Policies and Procedures Manual

Butte Countywide Homeless Continuum of Care

Adopted April 20, 2015

For use by the CoC Council, CoC Coordinator, HMIS Committee, HMIS Lead Agency, HMIS Software System Provider, Contributing HMIS Organizations, Partner Agencies, and all End Users

Table of Contents

I. Background

The U.S. Department of Housing and Urban Development ("HUD") uses Homeless Management Information System ("HMIS") data to inform homeless policy at the federal, state, and local levels. The HEARTH Act, enacted in 2009, requires that all recipients and subrecipients of Continuum of Care ("CoC") Program and Emergency Solutions Grant ("ESG") funds participate in their CoC's HMIS. The CoC Interim Rule (24 CFR 578) defines CoC HMIS responsibilities, including:

- Selecting an HMIS software solution
- Designating an eligible applicant to manage the HMIS (the "HMIS Lead Agency")
- Providing oversight for key HMIS policies
- Working with the HMIS Lead Agency to ensure consistent provider participation
- Ensuring the quality of HMIS data

In addition, the HMIS Proposed Rule (76 FR 22 76917) includes more specific HMIS requirements, including: the duties of the CoC; the duties of the HMIS Lead Agency; and security, data quality, privacy and technical standards.

With the Exception of Victim Service Providers defined by the Violence Against Women and Department of Justice Reauthorization Act of 2005 (Pub. L. 109-162) (VAWA), all homeless assistance programs that are a part of the Continuum of Care must participate in the HMIS, whether or not the specific program receives direct funding from HUD or other federal agencies. A particular program (or part of a program, such as a subset of beds within a program) is considered "participating" in HMIS if, as a matter of general practice, the program makes reasonable efforts to record all the Universal Data Elements for all clients served and discloses these data elements to the HMIS Lead Agency at least once annually. Disclosure may occur by directly entering data in the HMIS, electronically transferring data to the HMIS Lead Agency, or through other means determined with the HMIS Lead Agency. Such an HMIS participant is called a "Contributory HMIS Organization ("CHO")" in these HMIS Policies & Procedures.

The Butte Countywide Homeless Continuum of Care ("Butte CoC") Governance Charter, adopted by the Butte CoC Council, requires that the Butte CoC designate a legal entity that is also a Continuum of Care Program eligible applicant to serve as the Homeless Management Information System (HMIS) Lead Agency. The HMIS Lead Agency maintains Butte County's HMIS in compliance with HUD standards and coordinates all related activities, including training, maintenance and the provision of technical assistance to CHOs. More specific HMIS Lead Agency responsibilities are described in the HMIS Lead Agency Memorandum of Understanding (the "HMIS Lead Agency MOU") between the Community Action Agency of Butte County ("CAA") and the Butte CoC.

The Butte CoC *HMIS Policies and Procedures Manual* was created to outline how the Butte CoC will comply with the following regulations, standards and agreements: the HEARTH Act; CoC Interim Rule; HMIS Proposed Rule; HUD Data Standards (2014 HMIS Data Dictionary and 2014 HMIS Data Manual); Butte CoC Governance Charter; and HMIS Lead Agency MOU.

II. Definition of Terms

AHAR: Annual Homeless Assessment Report

APR: Annual Performance Report (formerly Annual Progress Report)

Butte CoC Council: The Butte CoC's governing body charged by the Butte CoC Governance Charter with planning and implementing HUD-funded efforts to end homelessness in Butte County

Butte CoC Governance Charter: The document that governs the roles, responsibilities and operations of the Butte CoC, Council, Committees, Lead Agency, Collaborative Applicant, and HMIS Lead Agency

CHO (Contributory HMIS Organization): An organization that enters data into the HMIS Software System in compliance with the CHO Participation Agreement and under the oversight of a CHO HMIS Administrator

CHO HMIS Administrator: A CHO staff person who is responsible for compliance with the CHO Participation Agreement and day-to-day operation of CHO data collection in HMIS

CHO Participation Agreement: An agreement entered into by the HMIS Lead Agency and CHO that describes the obligations and authority of the parties with regard to data collection, input, management and reporting

Client: A living individual about whom an Agency collects or maintains PPI

CoC: Continuum of Care

End User: An employee, volunteer, affiliate, associate, and any other individual acting on behalf of a CHO or HMIS Lead Agency who uses or enters data into the HMIS Software System or another administrative database from which data are periodically uploaded to the HMIS

HIC: Housing Inventory Chart

HMIS: Homeless Management Information System

HMIS Committee: Committee established by the Butte CoC Council to provide support and recommendations to the Butte CoC Council regarding HMIS policies and procedures; composed of staff representing the Butte CoC and HMIS Lead Agency, and all CHO HMIS Administrators

HMIS Software System: An HMIS data management software program developed and serviced by an HMIS Vendor

HMIS Lead Agency: An organization designated by a CoC to operate the CoC's HMIS

HMIS Vendor: Contractor who provides support services for the operation of a CoC's HMIS by contract, including the HMIS Software System provider, web server host, as well as providers of other contracted information technology or support

HUD: U.S. Department of Housing and Urban Development

NOFA: Notice of Funding Availability

PIT: Point in Time Count

PPI: Protected Personal Information

Security Officer: A staff person within the HMIS Lead Agency, and each CHO, that is responsible for their agency's compliance with the Security Plan of this *HMIS Policies and Procedures Manual*.

III. Roles and Responsibilities

1. Butte CoC Council

The Butte CoC Council is responsible for HMIS Project oversight and implementation, which encompasses planning, administration, software use, managing HMIS Data in compliance with HUD HMIS Standards, and reviewing and approving all policies, procedures, and data management plans governing CHOs. More specific Butte CoC Council responsibilities are listed below.

- Designate a single information system (the HMIS Software System) as the official HMIS software for the geographic area.
- Designate an HMIS Lead.
- Approve all HMIS policies, procedures and operational agreements.
- Develop a Governance Charter which includes a requirement that the HMIS Lead enter into written HMIS Participation Agreements with each Contributing HMIS Organization (CHO) and such additional requirements as may be issued by notice from time to time.

2. HMIS Committee

The HMIS Committee is designated by the Butte CoC Council to provide support and recommendations to the Butte CoC Council related to the HMIS regulations and standards as set forth by HUD. The HMIS Committee consists of staff representing the Butte CoC and HMIS Lead Agency, and all CHO HMIS Administrators.

3. HMIS Lead Agency

The HMIS Lead Agency manages HMIS data in compliance with HUD HMIS Standards, collects and organizes HMIS data within a data management software program (the "HMIS Software System"), and provides HMIS Project administrative functions at the direction of the Butte CoC, through its Butte CoC Council, and as further described in the HMIS Lead Agency MOU. Other principle responsibilities include:

Governance, Policy Development and Reporting

a) Draft policies, procedures and standards in accordance with the CoC Interim Rule, Proposed HMIS Rule, and 2014 HUD HMIS Data Standards;

b) Submit a security plan, data quality plan, and a privacy policy to the CoC for approval, to updated as needed;
c) Ensure implementation of policies, procedures and standards;
d) Ensure consistent participation by funding recipients;
e) Schedule and facilitate quarterly HMIS Committee meetings;
f) Prepare the following data reports and analyses for review by the Butte CoC Council and for submission to HUD: PIT Count; AHAR; HIC; unduplicated counts of clients served annually; count of lodging units in the HMIS; and other reports as necessary to measure progress in meeting Butte CoC goals;
g) Respond to CoC Council and HMIS Committee directives;
h) Work with the CoC Council to facilitate participation by all programs serving homeless people to participate in the HMIS;

System Administration and Security

i) Serve as the applicant to HUD for grant funds to be used for HMIS activities in the CoC's geographic area, and enter into grant agreements with HUD to carry out HUD-approved activities, as further described in the HMIS Lead Agency MOU;
j) Oversee the day-to-day administration of the HMIS system;
k) Manage the HMIS Software System Vendor and other HMIS Vendors in compliance with current HUD requirements and Proposed HMIS Rule technical standards;
l) Retain copies of all contracts and agreements executed for HMIS administration;
m) Designate a Security Officer responsible for ensuring compliance with applicable security standards, after conducting a criminal background check;
n) Require persons with access to all HMIS records to undergo a background check;
o) Keep all signed statements for a period of at least 3 years;
p) Implement a policy and chain of communication for reporting and responding to security incidents;
q) Develop a disaster recovery plan, which includes protocols for communication with staff, CoC and CHOs;
r) Complete an annual security review;

CHO and End User Coordination

s) Monitor and enforce compliance by all CHOs with HUD requirements and report on compliance to the CoC and HUD;
t) Communicate HUD HMIS Standards updates to all CHO HMIS Administrators;
u) Prepare and execute Participation Agreements with each CHO, which include
    a. The obligations and authority of the HMIS Lead Agency and CHO;
    b. The requirements of the Security Plan with which the CHO must abide;
    c. The sanctions for violating the Participation Agreement; and
    d. Agreement that the HMIS Lead Agency and CHO will process Protected Identifying Information consistent with the agreement;
v) Update contact list of all CHO HMIS Administrators in conjunction with annual Participation Agreement updates;
w) Manage and maintain mechanisms for soliciting, collecting and analyzing feedback from End Users, CHO HMIS Administrators, CHO Program Managers and Executive Directors, and homeless persons;
x) Document technical issues experienced by End Users;

Training and Technical Assistance

y) Develop and deliver a comprehensive training curriculum and protocol for CHO HMIS Administrators and End Users, as further described in the HMIS Lead Agency MOU;
z) Provide technical assistance and support to CHO HMIS Administrators and End Users;

Data Quality

aa) Develop and implement the Data Quality Plan;
bb) Establish data quality benchmarks for CHOs (calculated separately for: emergency shelter, safe haven, transitional housing and permanent housing), including bed coverage rates, service-volume coverage rates, missing/unknown value rates, timeliness criteria, and consistency criteria;
cc) Coordinate with CHO HMIS Administrators to produce required reports;
dd) Run and disseminate data quality reports on a quarterly basis to CHO programs indicating levels of data entry completion, consistency with program model, and timeliness;
ee) Provide quarterly reports on HMIS participation rates, data quality and other analyses to the Butte CoC Council and HMIS Committee;
ff) Monitor compliance by all CHOs with HMIS participation requirements, policies and procedures, privacy standards, security requirements, and data quality standards through an annual review per the process outlined in the Participation Agreement;
gg) Manage HMIS Software System upgrades and ensure that they comply with the latest HUD Data Standards; and
hh) Distribute HUD Data Standards and provide guidance to CHOs on compliance.

4. Contributing HMIS Organizations (CHOs)

CHOs operate a provider program and contribute Protected Personal Information or other client-level data to the HMIS Software System. CHOs must enter into and comply with CHO Participation Agreements in order to contribute such data to the HMIS Software System. Principle responsibilities described in this *HMIS Policies & Procedures Manual* include:

Data Quality

a) Collect the universal data elements, as defined by HUD, for all programs operated by the agency that primarily serve persons who are homeless or formerly homeless;
b) Collect program specific data elements, as defined by HUD, for all clients served by programs funded by HUD grants allocated to the Butte CoC;
c) Enter client-level data into the HMIS within seven days of client interaction;
d) Follow, comply and enforce the CHO Participation Agreement;

Security

e) Designate the HMIS Administrator as the Security Officer that is responsible for ensuring Security Plan compliance for the CHO;
f) Conduct criminal background checks, at a minimum based on a record review of the Superior Court records in the county of last residence, on the Security Officer and all End Users;
g) Ensure that all End Users receive security training prior to being given access to the HMIS, and once annually;

Privacy

h) Uphold confidentiality requirements;

i) Receive a Client Acknowledgement of Data Entry for each Client PPI entered into the HMIS Software System;
j) Post the HMIS Notice of Privacy Practices so that is viewable to all Clients; and

Training

k) Participate in comprehensive training curriculum developed by the HMIS Lead Agency;

5. CHO HMIS Administrator

A CHO HMIS Administrator is designated by each CHO to oversee day-to-day operation of its HMIS data collection system, ensuring program-level data quality according to the terms of the CHO Participation Agreement and associated Data Quality Plan, and managing data entry into the HMIS Software System. The CHO HMIS Administrator participates in quarterly HMIS Committee meetings and HMIS training meetings. Following are responsibilities with regard to Data Quality:

a) Be the first point of contact for End Users experiencing difficulties using HMIS;
b) Maintain End User list within the CHO;
c) Monitor End User logins on a monthly basis;
d) Complete data entry when End Users are unable to complete data entry;
e) Ensure CHO compliance with the protocols of the Data Quality Plan, Security Plan and Privacy Plan;
f) Inform the HMIS Lead Agency when critical deadlines regarding data entry are missed; and
g) Maintain communication with the HMIS Lead Agency and HMIS Committee regarding HMIS data entry challenges and questions.

6. HMIS Software System Vendor

The HMIS Software System Provider licenses and manages the HMIS software used by the Butte CoC by contract. The Butte CoC also requires the HMIS Software System Provider to:

a) Support the HMIS Lead Agency in providing training and technical assistance to the HMIS Lead Agency, CHO HMIS Administrators and End Users;
b) Encrypt data at the server level;
c) Revise HMIS Software System Provider software at the HMIS Lead Agency's request in order to comply with HUD HMIS Standards; and
d) Coordinate with the HMIS Lead Agency to add and remove End Users.

7. End User

a) Complete a classroom training with the HMIS Lead Agency and CHO HMIS Administrator, as required by the HMIS Lead Agency;
b) Maintain security of login and work station;
c) Follow data entry standards as required in the Data Quality Plan regarding completeness and timeliness;
d) Follow protocols as required by the Security Plan and Privacy Plan;
e) Ensure that paper documentation or physical files are complete;
f) Notify CHO HMIS Administrator if deadlines appear to be in jeopardy; and

g) Notify CHO HMIS Administrator with any questions, or if the HMIS Software System is not working properly.

IV. Data Quality Plan

1. Definition of Data Quality

Data quality refers to the extent that data recorded in the Butte CoC HMIS accurately reflects the same information in the real world. A perfect overlap between data and reality would result in a hypothetical data quality rating of 100%. While no data collection system has a quality rating of 100%, it is critical that the system provides the best possible representation of reality as it relates to homeless people and the programs that serve them. The overall goal is to record the most accurate, consistent and timely information in order to draw reasonable conclusions about the extent and impact of homelessness. All data entered into the HMIS Software System must comply with HUD's 2014 HMIS Data Standards.

One of the most effective ways to collect quality data is to develop data collection and data entry standards that are consistently implemented by all organizations and users entering data into the HMIS Software System. These standards will ensure that data is entered in a timely and consistent manner throughout the Butte CoC. The procedures and standards described below apply to all CHOs and End Users. CHO HMIS Administrators are responsible for ensuring that their organization's staff adheres to these procedures and standards.

2. Data Collection

Data Elements

Data Elements are the specific pieces of information that CHOs collect from clients and enter into the HMIS Software System. HUD's 2014 HMIS Data Standards (as defined in the HUD Data Standards Manual, Data Dictionary and HMIS Project Descriptor Data Elements Manual) govern the collection and input of Data Elements. The HMIS Lead Agency, CHOs and End Users must adhere to HUD's 2014 HMIS Data Standards. HUD may revise these standards from time to time in the future, at which point this *HMIS Policies and Procedures Manual* will need to be updated. Reference to HUD 2014 HMIS Data Standard guidance documents are provided in Section VIII Resources at the end of this *HMIS Policies and Procedures Manual*.

There are two Data Element categories— Universal and Program Specific. Universal Data Elements must be entered for all clients, regardless of funding source. Unlike Universal Data Elements, HUD does not require that all Program Specific Data Elements be collected for each client. Each CoC determines which Program Specific Data Elements to collect. The Universal Data Elements and Program Specific Data Elements are described in the 2014 Data Standards Manual, including data collection instructions, data element fields and response category descriptions.

Unique Client Identifier

A unique client identifier will be assigned by the HMIS to each client. The unique client identifier will not contain any masked client personal identifying information. The unique client identifier will not contain, in whole or in part, any client personal information as listed under Universal Data Elements. The unique client identifier provides an unduplicated internal count of clients served by the Agency, and provides the HMIS Lead Agency and HMIS Committee the means of conducting longitudinal analysis of services provided to each client.

3. Data Timeliness

Universal Data Elements, as defined by HUD's 2014 HMIS Data Standards, should be collected by CHOs from all clients at initial program enrollment. CHOs and Homeless Outreach Programs must enter data into the HMIS Software System within seven days of collecting the Client data elements. Program exit data should be entered on the same business day as exit. Homeless Outreach Programs also must enter data on all contacts made, date of engagement in outreach services, and dates of enrollment for specific programs (i.e. PATH). Please note that these expectations are subject to change.

4. Data Accuracy

Data accuracy is almost wholly dependent on the End User entering the correct information. In some cases, consistency checks can catch these errors. But for the most part, it is the responsibility of the End User to ensure that what is entered into the HMIS Software System reflects reality.

In addition to unintentional errors, the possibility of the Client providing false information always exists. It is impossible to completely eliminate all instances of intentionally false information. There are certain strategies to build trust and emphasize the benefits of accurate data to Clients. A firm understanding of why a client might provide false information, along with communicating to them the benefits of complete and accurate information, is a good start.

Reasons for providing false information:

- Privacy (not wanting to be tracked)
- Embarrassment/modesty
- A disability that results in paranoia
- Desire to qualify for service
- Fear of being turned away
- Not caring

Reasons for providing true information:

- Improved direct services
- Benefit eligibility and info validated
- Want to tell their story

- A relationship has been created
- Understand privacy/security procedures
- See benefits of HMIS for homelessness

In their explanation of the HMIS Notice of Privacy Practices and Client Acknowledgement of Data Entry documents, End Users should attempt to assuage any Client anxiety about providing information by explaining how they are designed to protect the Client's interest.

5. De-Duplication Procedures

The HMIS Software System software will use the following data elements to create deduplicated Client records:

- Name (first, middle, last, suffix, aliases or nicknames should be avoided);
- Social Security Number;
- Date of Birth (actual or estimated);
- Race and Ethnicity;
- Gender;
- Veteran's status; and
- Family status.

The primary way to achieve de-duplication will be a user-mediated search of the Client database prior to creating a new Client record. The End User will be prompted to enter a minimum number of the data elements into the HMIS application and a list of similar Client records will be displayed. Based on the results, the End User will be asked to select a matching record if the other identifying fields match correctly. If the End User is unsure of a match (either because some data elements differ or because of blank information), the End User should query the Client for more information and continue evaluating possible matches or create a new Client record.

The End User will not be able to view sensitive Client information, or program-specific information, during the de-duplication process. After the Client record is selected, the End User will only be able to view previously existing portions of the Client record if they have explicit authorization to view that Client's record.

6. Data Validity

For the purposes of this Data Quality Plan, Data Validity refers to all End Users defining and interpreting data elements the same way. The HMIS Committee reviews the definitions for each data element during training and these definitions and any updates are discussed at End User training meetings. If any End User has a question regarding how to define or interpret a data element they should feel free to contact the HMIS Lead Agency for direction. Some of the more frequently misinterpreted data elements and response categories are explored below.

Veterans – Adults (18 years or older) who have served active duty in any branch of the military. This includes the National Guard, but only if they were called up for active duty. Currently discharge status and time and place of service (e.g. Vietnam era) are not collected for most

programs, but may be in the future. Era of service, duration of service, discharge status, etc. is required for programs that serve Veterans only.

Chronically Homeless - An unaccompanied homeless individual with a disabling condition or an adult member of a homeless family who has a disabling condition and who has either been continuously homeless for 1 year or more, OR has had at least four episodes of homelessness in the past 3 years.

Literally Homeless – An individual or family who lacks a fixed, regular and adequate nighttime residence, meaning the individual or family has a primary nighttime residence that is a public or private place not meant for human habitation or is living in a publicly or privately operated shelter designed to provide temporary living arrangements. This category also includes individuals who are exiting an institution where he or she resided for 90 days or less who resided in an emergency shelter or place not meant for human habitation immediately prior to entry into the institution.

Imminent Risk of Homelessness – an individual or family who will imminently lose (within 14 days) their primary nighttime residence provided that no subsequent residence has been identified and the individual or family lacks the resources or support networks needed to obtain other permanent housing.

Housing Needed to Resolve Homelessness – This element refers to what the client will need to become stably housed in the long term. If their homelessness was caused by a short-term gap in employment, then an emergency shelter stay until their income is re-established may be the correct response. If a client's barriers are more severe, on-going rental assistance or permanent supportive housing may be the correct choice.

V. Security Plan

1. Hardware, Connectivity and Computer Security

Partner Agencies must have Internet connectivity for each workstation accessing the HMIS. To optimize performance, all agencies are encouraged to secure a high speed Internet connection with a cable modem, DSL, or T1 line. Agencies expecting a very low volume of data may be able to connect using a dial-up connection; however, HMIS management cannot guarantee satisfactory performance with this option.

Access to the HMIS will only be allowed from computers specifically identified by the CHO's Executive Director or authorized designee and the CHO HMIS Administrator. Laptop computers will require an additional security statement indicating that they will not be used for unauthorized purposes from unauthorized locations. Access to these workstations will be controlled through both physical security measures and a password. Each agency's CHO HMIS Administrator will determine the physical access controls appropriate for their organizational setting based on HMIS security policies, standards and guidelines.

All Participating agencies 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 the computers and data are secure and not usable by unauthorized individuals. Each computer must have password-protected screen savers. In addition, 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.

2. HMIS Lead Agency Implementation

Prior to setting up a new CHO to use the HMIS Software System, the HMIS Lead Agency shall:

a) Verify that the required documentation has been correctly executed and submitted or viewed on-site, including:

- Executed CHO Participation Agreement;
- Information Security Protocol;
- Designation of a CHO HMIS Administrator; and
- Designation of a Security Officer after conducting a criminal background check.

b) Request and receive approval from the HMIS Committee to setup a new agency;
c) Provide initial classroom training to the CHO HMIS Administrator and CHO End Users;
d) Work with the CHO HMIS Administrator to input applicable agency and program information; and
e) Work with the HMIS Committee to migrate legacy data, if applicable.

3. CHO Implementation

At a minimum, CHOs must develop rules, protocols or procedures to address the following:

- Internal agency procedures for complying with the HMIS Notice of Privacy Practices, the CHO Participation Agreement, the *HMIS Policies and Procedures Manual*, federal HMIS regulations, and HUD Standards;
- Maintaining and posting an updated copy of the HMIS Notice of Privacy Practices on the agency's website;
- Providing copies of the standard Client Acknowledgement of Data Entry to Clients;
- Appropriate assignment of End User accounts;
- Preventing End User account sharing;
- Protection of unattended workstations;
- Protection of physical access to workstations where employees are accessing HMIS;
- Safe storage and protected access to hardcopy and digitally generated client records and reports with identifiable client information;
- Proper cleansing of equipment prior to transfer or disposal; and
- Procedures for regularly auditing compliance with the *HMIS Policies and Procedures Manual*.

4. End User Implementation

Eligible End Users

Each CHO shall only authorize HMIS use to End Users who need access to the system for data entry and/or system administration. Data entry includes entering client records, editing client records, viewing client records, or other essential activity associated with carrying out CHO Participation Agreement responsibilities. System administration includes technical administration of the system, report writing, data analysis and report generation, back-up administration, activity associated with carrying out central server responsibilities, and other essential activity associated with carrying out CHO Participation Agreement responsibilities.

Setting Up New End Users

If the CHO wants to authorize system use for a new End User, the CHO's Executive Director or other authorized designee must:

a) Determine the appropriate access level of the End User; and
b) Execute an End User Agreement.

The CHO HMIS Administrator must:

a) Review HMIS records about previous End Users to ensure that the new End User does not have previous violations of HMIS Policy and Procedure that prohibit access;
b) Verify that the End User Agreement has been correctly executed;
c) Verify that initial classroom training with the HMIS Lead Agency and CHO HMIS Administrator has been successfully completed;
d) Coordinate with the HMIS Lead Agency to create the new End User ID and password; and
e) Manage End User accounts for the CHO, including removal of End Users.

End User Requirements

Prior to being granted a username and password, End Users must do the following:

a) Participate in a criminal background check;
b) Sign an HMIS End User Agreement that acknowledges receipt of the HMIS Policies and Procedures Manual and pledges compliance;
c) Receive initial classroom training with the HMIS Lead Agency and CHO HMIS Administrator, which includes awareness of the sensitivity of client-level data and appropriate measures to prevent its unauthorized disclosure; and
d) Receive a unique user name and password that is kept confidential.

Passwords

Each End User will be assigned a User ID, preferably the first and last name of the user. A temporary password will be automatically generated by the system when a new End User is created. The HMIS Lead Agency will communicate the system-generated password to the End User. The End User must establish a new password upon initial login. This password will need to be changed every 45? days. Passwords should be between 8 and 16 characters long, contain at least two numbers, and should not be easily guessed or found in a dictionary. The password format is alphanumeric and is case-sensitive. End Users are prohibited from sharing passwords—even with supervisors. Sanctions will be imposed on the End User and/or CHO if End User account sharing occurs. Any passwords written down should be securely stored and inaccessible to others. They should not be saved on a personal computer. An End User may only attempt to enter his/her password four times before the system inactivates that End User account. An End User account can only be reactivated by the HMIS Lead Agency.

Password Reset

In an End User has forgotten his/her password or for other reasons needs it to be changed, he/she must contact the HMIS Lead Agency by phone or email to request a new password. A password given by the HMIS Lead Agency is a temporary password and after entered once must be changed immediately by the End User.

End User Access Levels

The CHO HMIS Administrator will assign a designated End User access level to each End User that controls the level and type of access to the HMIS Software System. Each End User will only have access to client-level data that is collected by their own agency unless a client specifically consents in writing to share their information.

Changes to End User Accounts

Only the HMIS Lead Agency may make End User account changes. This includes adding or deleting an End User, changing passwords, upgrading or downgrading system privileges. If an End User account change must be made, the CHO HMIS Administrator must contact the HMIS Lead Agency within seven business days to request a change.

5. System Inactivity

End Users must logoff from the HMIS Software System and their workstation if they leave the workstation. Also, HUD requires password protected screen savers on each workstation. If the End User is logged onto a workstation and the period of inactivity on that workstation exceeds 30 minutes, the End User will be logged off the HMIS Software System automatically.

6. Electronic Data Control

CHOs must establish protocols limiting internal access to data based on HUD Data and Technical Standards.

Raw Data

End Users who have been granted access have the ability to download and save client level data onto their local computer. Once this information has been downloaded from the HMIS Software System in raw format to a CHO's computer, this data then becomes the responsibility of the CHO. Any such data files should be password protected.

Ability to Export Agency Specific Data from HMIS

CHOs will have the ability to export a copy of their own data for internal analysis and use. CHOs are responsible for the security of this information.

Data Storage

The HMIS Lead Agency and CHOs must store HMIS data for a minimum of seven years on a secure server.

7. Hard Copy Data Control

Printed hard copy versions of confidential data should not be copied or left unattended and open to compromise. Media containing HMIS client identified PPI data will not be shared with any agency, other than the owner of the data, for any reason. Authorized employees using methods deemed appropriate may transport HMIS data between the participating agencies that meet the above standard. Reasonable care should be taken, and media should be secured when left unattended. Magnetic media containing HMIS data should first be processed to destroy any data residing on that media. Degaussing and overwriting are acceptable methods of destroying data. HMIS information in hardcopy format should be disposed of properly. This could include shredding finely enough to ensure that the information is unrecoverable.

8. Enforcement Mechanisms

The HMIS Lead Agency and/or HMIS Committee will investigate all potential violations of any security protocols. Any End User found to be in violation of security protocols will be sanctioned.

Sanctions include, but are not limited to:

- A formal letter of reprimand
- Suspension of HMIS system privileges
- Revocation of system privileges

A CHO's access may also be suspended or revoked if serious or repeated violation(s) of this *HMIS Policy and Procedures Document*, as adopted by the Butte CoC, occur by the CHO's End Users.

VI. Privacy Plan

1. Client Notice

Each CHO must post or provide to each client a written notice of the assumed functions of the HMIS so that each client is aware of the potential use of his/her information and where it is stored (the "HMIS Notice of Privacy Practices"). If an agency maintains a public web page, the agency must post the HMIS Notice of Privacy Practices on its web page. No consent is required for the functions articulated in the notice. However, as part of the notification process, Clients must be informed of their right to designate his/her Client record as hidden/closed. This Client also has a right to view a copy of his/her record upon request. To fulfill this requirement, the CHO must post and adhere to the HMIS Notice of Privacy Practices. The HMIS Notice of Privacy Practices should be made available in languages common to the community, such as Spanish and Hmong.

Specific Client Notification Procedures for Victims of Domestic Violence

A mainstream agency that is serving a victim of domestic violence must explain the potential safety risks for domestic violence victims and the client's specific options to protect her/his data, such as designating her/his record as hidden/closed to other agencies. Thus, the HMIS Notice of Privacy Practices must clearly state the potential safety risks for domestic violence victims and delineate the information sharing options. All staff must be trained on the protocol for educating domestic violence victims about their individual information sharing options.

Specific Client Notification Procedures for Unaccompanied Minor Youth

Based on their age and potential inability to understand the implications of sharing information, the HMIS cannot be used to share information about unaccompanied minor youth outside of the originating agency. Thus, even with written Client authorization, End Users cannot share any Client information of unaccompanied minor youth. For the purposes of this policy, minor youth are defined as youth under 18.

2. Client Consent

Hidden/Closed Client Record

After learning about the HMIS, if a client does not wish to have his/her Primary Identifiers accessible to all HMIS users, the originating HMIS End User should close the client record by locking the security setting on the client screen. Closing a client record will allow the agency to access the client's information for agency purposes. This action will allow HMIS System Administrators to view client-identifying information, but will prevent any personal client-identifying information from being accessed by HMIS users outside of the originating agency.

Written Client Consent for Data Sharing

At the initial intake, the Client should be provided an oral explanation and written documentation about the option of sharing his/her Information within the CoC's HMIS. If a client is interested in sharing his/her information within the HMIS, he/she must provide written consent by signing the Client Acknowledgement of Data Entry. The client maintains a right to revoke written authorization at any time, in which case, any currently shared information will not be shared from that point forward.

Client Authorization

HMIS End Users may only share Client information if the Client authorizes that sharing with an executed Client Acknowledgement of Data Entry form. Authorized users will be able to grant permission based on appropriate Client consent to share individual client information with another agency's users. Random file checks for appropriate Client authorization, audit trails, and other monitoring tools may be used to monitor that this data sharing procedure is followed.

Applicability of Consent

The CHO shall uphold Federal and State Confidentiality regulations to protect client records and privacy. If an agency is covered by the Health Insurance Portability and Accountability Act (HIPAA), the HIPAA regulations prevail.

The table below summarizes the client data categories and the related notification/consent rules that relate to each data category. These minimum procedures should not imply that all providers would perform all of these functions.

Client Data Category	**Summary of Notification/Consent and Data Sharing Procedures**
Primary Identifiers Name and Aliases Birth Date Gender Social Security Number	Closed Client Record: If a client asks to hide his/her primary identifiers, the record will only appear on the Client Search List for the originating Agency. It will be hidden to all other agencies. Some System- level users will have access to hidden records for system administration purposes.
Open Client Record	If the Client does not ask to hide his/her Identifiers, the primary identifiers will be available to all HMIS users in the Client Search to locate an existing client. None of the other client information will be viewable, except as described below.
General Client Information:	
Ethnicity Race Veteran Status and Information Family/Relationship info Housing History Non Confidential Notes	Shared Record: With a signed Client Acknowledgement of Data Entry, these data can be shared with End Users from partnering agencies. Non-Shared Record: If written consent is not provided, this information is only accessible within the originating agency and some system-level End Users for system admin purposes.
Protected Information:	
Disability Information Mental Health Assessment Substance Abuse Assessment HIV/AIDS Information Domestic Violence Information	Generally, this information is only available within the original agency to End Users that have an authorized access level and to authorize system-level users for system admin purposes. Any other sharing of this Data should be limited to specific partner agencies as a closed exception and requires written consent from the client.

3. HMIS Data Release

Client Identifying Data

No identifiable Client data will be released to any person, agency, or organization that is not the owner of said data for any purpose other than those specified in this *HMIS Policies and Procedures Manual*, as adopted by the Butte CoC, without the written permission of the Client.

Data Release Criteria

HMIS Client data will only be released in aggregate, or in anonymous client-level data formats, for any purpose beyond those specified in this *HMIS Policies and Procedures Manual*, as adopted by the Butte CoC, according to the criteria specified below.

Aggregate Data Release Criteria

All HMIS 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. Aggregate Data must represent sixty percent (60%) of the total Clients being served by the CoC (program, agency, subpopulation, geographic area, etc.), unless otherwise required for the Congressional Annual Homeless Assessment Report (AHAR).

Only CHOs can authorize release of aggregate program-specific information beyond the standard reports compiled by the Alliance for funding purposes. There will be full access to aggregate data for all participating agencies.

Parameters of the release of aggregate data (i.e., where the data comes from, what it includes and what it does not include) will be presented to each requestor of aggregate data. Released aggregate data will be made available in the form of an aggregate report, and/or a raw dataset.

Data Release Process

Beyond individual agency reports, or CoC reports on its funded programs, the Butte CoC Chair must approve all data for public classification and release.

4. Privacy Compliance and Grievance Policy

CHOs must establish a regular process of training End Users on Privacy Plan compliance, regularly auditing that the Privacy Plan is being followed by CHO staff (including employees, volunteers, affiliates, contractors and associates), and receiving and reviewing complaints about potential violations of the policy.

VII. Technical Standards

The HMIS Lead Agency will ensure that the HMIS Software System:

- Contains fields for collection of all data elements established by HUD notice.
- Record data from a theoretically limitless number of service transactions while following federal, state, territorial, or local data retention laws and ordinances.
- Generates the report outputs specified by HUD, including representation of dates for all historical and transactional data elements.
- Produces reports that enable the CHOs and HMIS Lead Agency to assess compliance with HUD data quality benchmarks.
- Generates audit reports that allow the HMIS Lead Agency to review the audit logs on demand, including HUD data requirements.

VIII. Resources

Regulations and Requirements

HEARTH Act of 2009, S. 896 (https://www.hudexchange.info/resource/1715/mckinney-vento-homeless-assistance-act-amended-by-hearth-act-of-2009/)

CoC Program Interim Rule, 25 CFR Part 578
(https://www.hudexchange.info/resource/2033/hearth-coc-program-interim-rule/)

HMIS Requirements Proposed Rule, 76 FR 22 76917
(https://www.hudexchange.info/resource/1967/hearth-proposed-rule-for-hmis-requirements/)

2014 HMIS Data Standards

HMIS Data Standards Manual, U.S. Dept. of Housing and Urban Development
(https://www.hudexchange.info/resource/3826/hmis-data-standards-manual/)

HMIS Data Dictionary, U.S. Dept. of Housing and Urban Development
(https://www.hudexchange.info/resource/3824/hmis-data-dictionary/)

Guides and Tools

2014 HMIS Data Standards Mapping, U.S. Dept. of Housing and Urban Development
(https://www.hudexchange.info/resource/4052/2014-hmis-data-standards-mapping/)

HMIS Project Descriptor Data Elements Manual, U.S. Dept. of Housing and Urban Development
(https://www.hudexchange.info/resource/4055/hmis-project-descriptor-data-elements-manual/)