Butte Countywide Homeless Continuum of Care

Homeless Management Information System / Coordinated Entry Committee
Monday, September 9, 1:00 p.m. – 3:00 p.m.
Butte County Employment and Social Services – Teams Virtual Meeting
Teams Meeting: Please use the Meeting ID and Passcode to join the meeting.
Phone: (332) 249-0500 Meeting ID: 255 420 652 955 Passcode: pG4YhE

HMIS/CE COMMITTEE MEMBERS (CHO Administrator, or designee):

Angie Little, HACB
Codie McCormack, Caminar
Nancy Jorth, Youth for Change
Susan Wilson, Safe Space
Brian Boyer, CAA
Yesenia Gallegos, CHAT
Cynthia Pesheck, Ampla
Cathryn Carkhuff, Home & Heart
Rayna Bryson, DESS HSP
Lisa Torres OSCIA
Shelly Watson, Jesus Center
Tracey Gilliham, Butte 211
TBD, BCDBH
Ann Winters, Catalyst
Debbie Villasenor, Consultant
Elisa Rawlinson, DESS HHOME
Jaymee McLaughlin, CUSDD
Karen Ramirez, True North Housing Alliance
Lynann Pilley, Oroville Rescue Mission
Kim Decker, Nation's Finest
Nick Fashing, DESS APS
Halle Brown, NCIHA
Josh Indar, BCOE
Maisue Thao, Butte College

First Chairperson: Elisa Rawlinson, DESS HH **Second Chairperson:** Sarah Frohock, BCDBH

AGENDA

1. Call to Order — Elisa
2. Introductions — All
3. Training — Elisa
   a. VI-SPDAT (upcoming changes)
4. Night-by-Night Shelters, Exiting Policy ***- DISCUSSION and APPROVAL*** — ***All***
5. HMIS Privacy & Security Plan- ***DISCUSSION*** — ***All***
6. Scheduling Special Meeting (September 30, 2024, 1pm - 3pm) — All
7. Agency Announcements — All
8. Next Meeting:
   Monday, September 30, 2024; 1:00 – 3:00 p.m. (Special Meeting)
   Monday, October 7, 2024; 1:00 - 3:00 p.m.
9. Adjourn

Emergency Shelter Exit Date Guidance

Shelter Type	Stay Details	Project Exit Date	Example
Night-by-night Shelter Client's project exit date is recorded as the day after the last bed night date.	**Scenario 1: Regular Stay**		
	First bed night: January 1, 2023	The client's project exit date is January 4, 2023 (The day after the last bed night).	First bed night: January 1, 2023 Last bed night: January 3, 2023 Exit date: January 4, 2023
	Last bed night: January 3, 2023		
	Scenario 2: Irregular Stay		
	First bed night: January 1, 2023	After the first absence: The client's project exit date is January 11, 2023 (The day after the last bed night).	First bed night: January 1, 2023 Last bed night before a break: January 10, 2023
	Last bed night before a break: January 10, 2023		Client returns: January 15, 2023
	Client returns: January 15, 2023		
	Last bed night: January 20, 2023	After the second stay: The client's project exit date is January 21, 2023 (The day after the last bed night).	Last bed night: January 20, 2023 Exit date: January 21, 2023

Emergency Shelter Exit Date Guidance

Determining the Project Exit Date for Night-by-Night Shelter Stays

In night-by-night emergency shelters, the client's project exit date is recorded as the day after the last bed night date. Here are two scenarios using the same dates as in the most recent chart:

Scenario 1: Regular Stay

- Client's Stay Details:

- First bed night: January 1, 2023
- Last bed night: January 3, 2023

- Exit Date Determination:

- The client's project exit date is January 4, 2023 (the day after the last bed night).

Scenario 2: Irregular Stay

- Client's Stay Details:

- First bed night: January 1, 2023
- Last bed night before a break: January 10, 2023
- Client returns: January 15, 2023
- Last bed night: January 20, 2023

- Exit Date Determination:

- After the first absence: The client's project exit date is January 11, 2023 (the day after the last bed night).
- After the second stay: The client's project exit date is January 21, 2023 (the day after the last bed night).

Key Points:

- For night-by-night emergency shelters, the exit date is always the day after the last bed night.
- This method ensures accurate tracking of client stays and supports streamlined data collection and reporting.

Emergency Shelter Exit Date Guidance

Shelter Type	Stay Details	Project Exit Date	Example
Entry/Exit Shelter Client's project exit date is recorded as the last day of a continuous stay in the project.	**Scenario 1: Continuous Stay**		
	Project entry date: January 1, 2023	The client's project exit date is January 10, 2023 (The last day of their continuous stay).	Project entry date: January 1, 2023 Last day in the shelter: January 10, 2023 Exit date: January 10, 2023
	Last day in the shelter: January 10, 2023		
	Scenario 2: Extended Stay with Transfer		
	Project entry date: February 1, 2023	The client's project exit date is February 15, 2023 (The last day of their continuous stay before transferring).	Project entry date: February 1, 2023 Last day before transfer: February 15, 2023 Exit date: February 15, 2023
	Client stays continuously until February 15, 2023		
	Client transfers to another shelter on February 15, 2023		

Emergency Shelter Exit Date Guidance

Determining the Project Exit Date for Entry/Exit Shelters

In entry/exit emergency shelters, the client's project exit date is recorded as the last day of their continuous stay in the project. Here are two scenarios using the same dates as in the previous chart:

Scenario 1: Continuous Stay

- Client's Stay Details:

- Project entry date: January 1, 2023

- Last day in the shelter: January 10, 2023

- **Exit Date Determination:**

- The client's project exit date is January 10, 2023 (the last day of their continuous stay).

Scenario 2: Extended Stay with Transfer

- Client's Stay Details:

- Project entry date: February 1, 2023

- Client stays continuously until February 15, 2023

- Client transfers to another shelter on February 15, 2023

- **Exit Date Determination:**

- The client's project exit date is February 15, 2023 (the last day of their continuous stay before transferring to another residential project).

Key Points:

- For entry/exit emergency shelters, the exit date is the last day the client resides continuously in the project.

- Transfers to another residential project are considered the exit date for the original shelter.

This method ensures accurate tracking of client stays and supports streamlined data collection and reporting.

Proposed addendum to the Butte Countywide Homeless Continuum of Care's
HMIS Policy and Procedure: Exiting Clients from Night-by-Night Emergency Shelters
(This would be added under the "Bed/Unit Utilization Rates" section of the HMIS P&Ps)

Automatic Exits from Night-by-Night Emergency Shelters

The U.S. Department of Housing and Urban Development (HUD) recognizes two types of emergency shelters: "Entry Exit" (EE) and "Night-by-Night" (NbN). Reporting and outcomes vary based on the shelter type.

- EE Shelter Projects: Require a full client record for each stay, with all necessary data recorded at both entry and exit.
- NbN Shelter Projects: Require a full client record followed by a record for each night the client stays.

In NbN shelters, HMIS end users must complete all exit data elements for clients whenever possible. Clients known to be housed or no longer participating in the project should be manually exited. HUD guidelines suggest CoCs establish a standard for "automatic exits" after a specified period of absence. This system simplifies data collection for large shelters while still promoting complete exit information.

The CoC, with assistance from the HMIS/CES Committee, has decided that clients in NbN ES projects will be considered exited if they have _____ consecutive days with no recorded bed nights. The local HMIS will automatically exit the client, with the exit date being the day after their last tracked bed night.

Temporary Exits from Emergency Shelters

Sometimes, clients are asked to leave an ES project for a predetermined period due a variety of reasons. Locally, it has been decided that when a client is asked to leave, other shelters should support this decision and prevent "shelter hopping."

When an ES project asks a client to leave temporarily, ES staff must, within 4 hours, enter a Public Alert in the client's profile, indicating:

- The date the client was asked to leave; and
- The number of days the client has been temporarily exited from the shelter; and
- The date the client is allowed to return to the shelter.

The alert should be set to expire the same day as the client's allowable return date. The alert should not include any indication related to the reason the client was asked to temporarily leave the project, unless the client was determined to be a safety concern. If the client has been determined to be a possible safety risk, the alert must indicate the client is a potential safety risk to staff or other clients.

Additionally, staff must exit the client from the ES project with an exit date that complies with HUD regulations.

Current Public Notice

Butte Countywide Homeless Information Systems (HMIS) Public Notice

We collect personal information directly from you to:

1. *Best connect you with the services you need;*
2. *Better understand the needs of homeless persons;*
3. *Improve planning to eliminate homelessness; and*
4. *Improve services for homeless persons.*

The only people who will be allowed to see your information are HMIS trained staff for homeless service providers who have agreed to keep your information confidential. Additional details regarding data collection and sharing are discussed in our Privacy Notice. If you would like a copy of our Privacy Notice, please ask.

Current Privacy Notice

Butte Countywide Continuum of Care
Privacy Notice

Adopted November 16, 2020

A. Scope of Notice

1. This notice describes the privacy policy and practices of Butte Countywide Homeless Continuum of Care (Butte CoC) and Name of Homeless Organization, a Contributing HMIS Organization (CHO). Our main office is at Address, email/web address,telephone of Homeless Organization.
2. A Homeless Management Information System (HMIS) is a software system used to collect data on the housing and services provided to homeless individuals and families and persons at risk of homelessness. All homeless assistance programs that are a part of the Butte CoC must participate in the HMIS, and are called Contributing HMIS Organizations (CHOs). CHO's are required to collect universal data elements from all clients, including Protected Personal Information (PPI).
3. The policy and practices in this notice cover the processing of PPI HMIS for clients of Name of Homeless Organization.
4. Protected Personal information (PPI) is any information we maintain about a client that:
   a. allows identification of an individual directly or indirectly
   b. can be manipulated by a reasonably foreseeable method to identify a specific individual or
   c. can be linked with other available information to identify a specific client
5. When this notice refers to personal information, it means PPI.
6. All personal information that we maintain is covered by the policy and practices described in this privacy notice. if programs provided by your agency have additional privacy requirements, please add that information here: for example " Personal information that the medical clinic collects and maintains is covered by a different privacy policy". Or Delete this text.
7. We adopted this policy because of standards for HMIS issued by the Department of Housing and Urban Development. We intend our policy and practices to be consistent with those standards. See 69 Federal Register 45888 (July 30, 2004).
8. This notice tells our clients, our staff, and others how we process personal information. We follow the policy and practices described in this notice.
9. We may amend this notice and change our policy or practices at any time. Amendments may affect personal information that we obtained before the effective date of the amendment.
10. We give a written copy of this privacy notice to any individual who asks.

11. A copy of this notice can be found on the HMIS/CES page of the Butte CoC website at www.buttehomelesscoc.com

B. Data Collection and Purpose

1. We collect personal information only when appropriate to provide services or for another specific purpose of our organization or when required by law. We may collect information for these purposes:
   a. to provide or coordinate services to clients
   b. to locate other programs that may be able to assist clients
   c. for functions related to payment or reimbursement from others for services that we provide
   d. to operate our organization, including administrative functions such as legal, audits, personnel, oversight, and management functions
   e. to comply with government reporting obligations
   f. when required by law

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

3. We normally collect personal information with the knowledge or consent of our clients. If you seek our assistance and provide us with personal information, we assume that you consent to the collection of information as described in this notice.
4. We may also get information about you from other CHOs within the Butte CoC.
5. We post a sign at our intake desk or other location explaining the reasons we ask for personal information. The sign says:

   We collect personal information directly from you to:
   1. Best connect you with the services you need;
   2. Better understand the needs of homeless persons;
   3. Improve planning to eliminate homelessness; and
   4. Improve services for homeless persons.

   The only people who will be allowed to see your information are HMIS trained staff for homeless service providers who have agreed to keep your information confidential. Additional details regarding data collection and sharing are discussed in our Privacy Notice. If you would like a copy of our Privacy Notice, please ask.

C. Permitted Uses and Disclosures

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

a. to connect individuals to appropriate resources or services, for housing prioritization purposes, and for determining an individual's progress in programs or services
b. for functions related to payment or reimbursement for services
c. to carry out administrative functions such as legal, audits, personnel, oversight, and management functions
d. to create de-identified (anonymous) information that can be used for research and statistical purposes without identifying clients
e. when required by law to the extent that use or disclosure complies with and is limited to the requirements of the law
f. to avert a serious threat to health or safety if
   (1) we believe that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public, and
   (2) the use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat
g. to report about an individual we reasonably believe to be a victim of abuse, neglect or domestic violence to a governmental authority (including a social service or protective services agency) authorized by law to receive reports of abuse, neglect or domestic violence
   (1) under any of these circumstances:
      (a) where the disclosure is required by law and the disclosure complies with and is limited to the requirements of the law
      (b) if the individual agrees to the disclosure, or
      (c) to the extent that the disclosure is expressly authorized by statute or regulation, and
         (I) we believe the disclosure is necessary to prevent serious harm to the individual or other potential victims, or
         (II) if the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the PPI for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

   and
   (2) when we make a permitted disclosure about a victim of abuse, neglect or domestic violence, we will promptly inform the individual who is the victim that a disclosure has been or will be made, except if:
      (a) we, in the exercise of professional judgment, believe informing the individual would place the individual at risk of serious harm, **or**
      (b) we would be informing a personal representative (such as a family member or friend), and we reasonably believe the personal representative is responsible for the abuse, neglect or other injury, and that informing the personal representative would not be in the best interests of the individual as we determine in the exercise of professional judgment.
h. for academic research purposes
   (1) conducted by an individual or institution that has a formal relationship with the CHO if the research is conducted either:

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

and

(2) any written research agreement:
(a) must establish rules and limitations for the processing and security of PPI in the course of the research
(b) must provide for the return or proper disposal of all PPI at the conclusion of the research
(c) must restrict additional use or disclosure of PPI, except where required by law
(d) must require that the recipient of data formally agree to comply with all terms and conditions of the agreement, and
(e) is not a substitute for approval (if appropriate) of a research project by an Institutional Review Board, Privacy Board or other applicable human subjects protection institution.

i. to a law enforcement official for a law enforcement purpose (if consistent with applicable law and standards of ethical conduct) under any of these circumstances:
(1) in response to a lawful court order, court-ordered warrant, subpoena or summons issued by a judicial officer, or a grand jury subpoena
(2) if the law enforcement official makes a written request for PPI that:
(a) is signed by a supervisory official of the law enforcement agency seeking the PPI
(b) states that the information is relevant and material to a legitimate law enforcement investigation
(c) identifies the PPI sought
(d) is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought, and
(e) states that de-identified information could not be used to accomplish the purpose of the disclosure.
(3) if we believe in good faith that the PPI constitutes evidence of criminal conduct that occurred on our premises
(4) in response to an oral request for the purpose of identifying or locating a suspect, fugitive, material witness or missing person and the PPI disclosed consists only of name, address, date of birth, place of birth, Social Security Number, and distinguishing physical characteristics, or
(5) if
(a) the official is an authorized federal official seeking PPI for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879 (threats against the President and others), and
(b) the information requested is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought.

and

j. to comply with government reporting obligations for homeless management information systems and for oversight of compliance with homeless management information system requirements.

2. Before we make any use or disclosure of your personal information that is not described here, we seek your consent first.

D. Client Control Over Data

1. You may inspect and have a copy of your personal information that we maintain. We will offer to explain any information that you may not understand.
2. We will consider a request from you for correction of inaccurate or incomplete personal information that we maintain about you. If we agree that the information is inaccurate or incomplete, we may delete it or we may choose to mark it as inaccurate or incomplete and to supplement it with additional information.
3. To inspect, get a copy of, or ask for correction of your information, ask an agency staff member for assistance, contact this organization at Address, email/web address, telephone of Homeless Organization, or email ButteCoC@buttecounty.net.
4. We may deny your request for inspection or copying of personal information if:
   a. the information was compiled in reasonable anticipation of litigation or comparable proceedings
   b. the information is about another individual (other than a health care provider or homeless provider)
   c. the information was obtained under a promise or confidentiality (other than a promise from a health care provider or homeless provider) and if the disclosure would reveal the source of the information, **or**
   d. disclosure of the information would be reasonably likely to endanger the life or physical safety of any individual.
5. If we deny a request for access or correction, we will explain the reason for the denial. We will also include, as part of the personal information that we maintain, documentation of the request and the reason for the denial.
6. We may reject repeated or harassing requests for access or correction.

E. Data Quality

1. We collect only personal information that is relevant to the purposes for which we plan to use it. To the extent necessary for those purposes, we seek to maintain only personal information that is accurate, complete, and timely.
2. We have a plan to dispose of personal information not in current use seven years after the information was created or last changed. As an alternative to disposal, we may choose to remove identifiers from the information.

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

F. Complaints and Accountability

1. We accept and consider questions or complaints about our privacy and security policies and practices. You can complain about our privacy and security policies by writing to: Butte County DESS Housing and Homeless Branch, 202 Mira Loma Drive, Oroville, CA 95965 or e-mailing ButteCoC@buttecounty.net. You will receive a response in writing postmarked or date stamped within five working days if a valid email address or mailing address is provided in the written complaint.
2. All members of our staff (including employees, volunteers, affiliates, contractors and associates) are required to comply with this privacy notice. Each staff member must receive and acknowledge receipt of a copy of this privacy notice.

G. Privacy Notice Change History

1. Version 1.0, 11-16-2020, Initial Policy

Proposed
HMIS Privacy & Security Plan

HMIS Privacy and Security Plan

Butte Countywide Homeless Continuum of Care

PRIVACY & SECURITY

Privacy refers to the protection of a client's data stored in HMIS from open viewing, sharing or inappropriate use.

Security refers to the protection of a client's data stored in HMIS from unauthorized access, use or modification.

Created July 23, 2024
Approved on _____

Table of Contents

Contents

Introduction

A Homeless Management Information System (HMIS) contains highly sensitive medical, financial, and personal data ranging from substance abuse treatment and mental health records to immigration status. In a world rife with cyberattacks, such private information must always be treated as at risk—especially for already vulnerable populations experiencing homelessness.

Data breaches come with significant safety and security risks. For example, stolen information can worsen the financial situation of people experiencing homelessness, while knowing other people have acquired private life details without consent can undermine a person's feelings of safety and autonomy.

To protect individuals against privacy violations and data security breaches, all HMISs are subject to HIPAA, 42 Code of Federal Regulations (CFR) Part II, and other regulations. For instance, HIPAA is a federal law requiring that no sensitive health information be disclosed without a patient's consent or knowledge.

HMIS is a trust-based system. In other words, clients are putting a great deal of faith into the hands of care providers and case managers when they share the private details of their lives with them. Additionally, one of the main purposes of HMIS is for service providers to take the burden of "keeper of data" off of clients who are living in crisis and onto themselves. Thus, allowing clients to focus survival, healing and ultimately housed self-sufficiency.

Most Continuums of Care (CoCs) rely primarily on self-reported data from clients. Individuals experiencing homelessness who don't trust the security and privacy of HMIS and of the Contributing HMIS Organization (CHO) will be reluctant to answer candidly, which ultimately hinders the CHO's ability to provide the tailored help client's need - and will undermine the reliability of the data. Success with clients hinges on trust.

Background

The following HUD HMIS Standards were referenced in the creation of this document:

- 2004 HMIS Data and Technical Standards Final Notice
- 2010 HMIS Data Standards Revised Notice: released on March 29, 2010. These final Standards reflect the public comments that HUD received on a set of draft Data Standards, which were released in July 2009. They incorporate the interim Data Standards for the Homelessness Prevention and Rapid Re-Housing Program (HPRP) published in June 2009, and replace Sections 2 (Universal Data Elements) and Section 3 (Program-Specific Data Elements) of the 2004 HMIS Data and Technical Standards. All other sections of the 2004 notice, such as the privacy and security standards, remain in effect.
    - HMIS Data standards are updated biannually (every two years). As of the writing and approval of this plan the most recently released Data Standards are the 2024 HMIS Data Standards. These Data Standards update data collection rules and definitions as they relate to HMIS, however all other sections of the 2004 notice, such as the privacy and security standards, remain in effect.
- 2011 HMIS Requirements Proposed Rule

- Starting in 2014 HUD has changed both the format and the contents of the information. Rather than compiling all the information into one document HUD is releasing a series of documents designed for specific audiences. They are:

- **HMIS Data Dictionary** – The HMIS Data Dictionary is designed for HMIS vendors and HMIS Lead Agency system administrators to understand all of the data elements required in an HMIS, data collection and function of each required element and the specific use of each element by the appropriate federal partner. The HMIS Data Dictionary should be the source for HMIS software programming.
- **HMIS Data Manual** – The HMIS Data Manual is designed for HMIS Lead Agency system administrators, Continuum of Care leaders, and HMIS users. The Manual lists and defines data elements to be collected in an HMIS and provides definitions and program use context for data collection. Identical data elements are presented in the Data Dictionary and Data Manual but the readership and context are different.
- **HMIS Program Manuals** – A series of program manuals will be released prior to October 1, 2014. These manuals will enable an HMIS to be used across all of the federal partners identified in the Data Dictionary and the Data Manual. The Manual will provide HMIS Leads, HMIS vendors, CoCs, and end users with all of the information they need on each federal partners specific programs and program components.

The HMIS Lead Agency oversees the overall privacy and security of the local HMIS. The HMIS Lead Agency and HMIS Lead Agency System Administrator is responsible for preventing degradation of HMIS resulting from viruses, intrusion, or other factors within the HMIS Lead Agency System Administrator's control and for preventing inadvertent release of confidential client-specific information through physical, electronic or visual access to Administrator workstations or system servers. However, CHOs play a crucial role in protecting HMIS.

CHOs are responsible for ensuring their systems are secure from viruses, unauthorized access, and other threats within their control. CHOs must also take measures to prevent the release of confidential client information through verbal, physical, electronic, or visual access to their workstations, devices or paperwork.

Each CHO must adhere to the Privacy and Security requirements set by the HUD 2004 HMIS Data and Technical Standards. This includes conducting a thorough review of their internal policies and procedures related to HMIS privacy and security on a quarterly basis. By doing so, CHOs help maintain the integrity and confidentiality of HMIS.

Privacy

Plan Overview

On July 30, 2004, the US Department of Housing and Urban Development (HUD) released the HMIS standards (69 Federal Register No. 146). On December 9, 2011 HUD released HMIS Requirements Proposed Rule (Federal Register / Vol. 76, No. 237)**.** These standards outline the responsibilities of HMIS, the Lead Agency and CHOs.

This section describes the Privacy Plan of the Butte Countywide HMIS System. The policies and information contained within this plan are consistent with HUD standards. All HMIS End Users, CHOs, CHO staff and system administrators must adhere to this Privacy Plan. Failure to comply may result in the removal of an End User or CHO Agency from the HMIS.

This document supports the Butte Countywide Continuum of Care's (CoC) aim of providing an effective and usable case management tool that helps clients move through the homeless service system in a safe, secure, caring and trauma-informed manner. The CoC recognizes clients served by individual agencies are not exclusively that "agency's client" but instead are truly a client of the Butte Countywide CoC. Therefore, this Privacy Plan supports an open system of client-level data sharing amongst agencies.

The core tenant of the Privacy Plan is the Baseline Privacy Notice (which can be found in Appendix A of this document, herein referred to as the "Privacy Notice" which was approved by the CoC the same date as this plan was adopted and approved. This notice describes how client's information may be used and disclosed and how clients can access their information. Each agency must, at minimum, adopt the Privacy Notice approved by the CoC. If a CHO is subject to higher levels of privacy and security standards due to the nature of their homeless population, service provisions, grant requirement or other federal or state regulation, they must develop a Privacy Notice which exceeds all minimum requirements set forth in the CoC approved Privacy Notice (this is described in the Agency Responsibilities section of this Privacy Plan). This ensures all agencies participating in HMIS are governed by the same minimum standards of client privacy protection. Any CHO who develops a Privacy Notice that exceeds the minimum requirements set forth in the CoC approved Privacy Notice, must provide a copy to the HMIS/CES Committee and the CoC for approval.

All CHOs must post either the CoC's approved Privacy Notice their own CoC approved Privacy Notice on their agency's local website (if available).

All individuals with access to Personal Protected Information (PPI/PII), also known as Personal Identifying Information (PII), herein referred to PPI/PII, are required to complete formal training in privacy requirements at least annually.

The Privacy Notice may be amended at any time. Amendments may affect information obtained by the agency before the date of the change. An amendment to the Privacy Notice regarding use or disclosure will be effective with respect to information processed before the amendment, unless otherwise stated. A record of all amendments to this Privacy Notice must be made available to clients upon request.

This document reflects the baseline requirements listed in the HMIS Data and Technical Standards Final Notice, published by HUD in July 2004. Should any inconsistencies with the HUD Standards be identified, please immediately notify the Butte Countywide HMIS Lead Agency, using the contact information below, and note the HUD Standards take precedence.

All questions and requests related to this Privacy Notice should be directed to: HMIS Lead with Butte County Department of Employment and Social Services (DESS): HMIShelp@buttecounty.net or 530-552-6200 and ask for the HMIS Lead.

Privacy Notice: This is the main document of this Privacy Plan. This document outlines the minimum standard by which an agency collects, utilizes and discloses information.	*__REQUIRED__* Agencies must, at minimum, adopt the Privacy Notice approved by the CoC, which meets all minimum standards set forth by HUD. CHOs must post the CoC approved Privacy Notice on the Agency's local website (if available).
Public Notice: This posting explains the reason for asking for personal information and notifies the client of the Privacy Notice.	*REQUIRED* Agencies must adopt and utilize the Public Notice. This notice must be posted, and easily visible at any station or place in which HMIS data is gathered from clients. Including while conducting outreach.
Informed Consent: This form must be signed by all adult clients and unaccompanied youth. This gives the client the opportunity to refuse the sharing of their information with other agencies within the system. Parents with underage children who are either in their physical care and custody or whose children are expected to live with the parent upon receipt of housing, must include all children's names on the Informed Consent.	*__REQUIRED__* Client Signatures or Verbal Approval are required prior to inputting client information in HMIS.

HMIS User Responsibilities

A client's privacy is upheld only to the extent that HMIS users, CHOs, HMIS End Users and CHO staff protect and maintain said privacy. The role and responsibilities of the HMIS End User cannot be over-stated.

"CHO staff" is defined as a person that has direct interaction with a client or their HMIS data, regardless of whether or not they are entering the data into HMIS. (This could potentially be any person at the agency: staff member, volunteer, contractor, etc.) All CHO staff have the responsibility to:

- Understand the Butte Countywide CoC's HMIS Privacy Notice
- Be able to explain the Privacy Notice to clients
- Follow the Privacy Notice
- Know where or to whom they should refer the client if they cannot answer the client's questions
- Complete an **Informed Consent** with client prior collecting HMIS data (if there is not

already an active Informed Consent in the system, or if the client is new to HMIS)

- Provide client a copy of the "Privacy Notice Quick Guide for Organizations in the Butte Countywide Homeless Continuum of Care"
- Collect client HMIS data in a place/location in which the Public Notice is easily visible to the client
- If a client requests a copy of the Privacy Notice it must be provided to client before collecting any information.
    - The client must sign the Acknowledgment of Receipt, and a copy must be uploaded to the client level file.
- Uphold the client's privacy in the HMIS and surrounding their data, information, or story as it relates to HMIS.

Agency Responsibilities

The 2004 HUD HMIS Standards emphasize it is the CHO's responsibility to uphold client privacy. CHOs and CHO staff must understand the legal, ethical and regulatory responsibilities of collecting and maintaining client data. This policy and the Privacy Notice provide guidance on the minimum standards by which CHOs and CHO staff must operate if they wish to participate in the HMIS.

Meeting the minimum standards in this Privacy Plan and the Privacy Notice are required for participation in the HMIS. Any agency may exceed the minimum standards described. Agencies must adopt the Butte Countywide CoC HMIS Privacy Notice which meets the minimum standards before data entry into the HMIS can occur.

CHOs have the responsibility to:

- Review their program requirements to determine what industry privacy standards must be met that exceed the minimum standards outlined in this Privacy Plan and Privacy Notice (examples: Substance Abuse Providers covered by 24 CFR Part 2, HIPPA Covered Agencies, Legal Service Providers).
- Review the 2004 HUD HMIS Privacy Standards (69 Federal Register 45888)
- Adopt and uphold the Privacy Notice which meets all minimum standards in the Privacy Notice as well as all industry privacy standards. Modifications to the Privacy Notice must be approved by the HMIS Committee and then approved by the Butte Countywide CoC.
- Ensure that all CHO staff are aware of the Privacy Notice and have access to it. If the agency has a website, the agency must publish the Privacy Notice on their website.
- Make reasonable accommodations for persons with disabilities, language barriers or education barriers.
- Ensure that anyone working with clients covered by the Privacy Notice can meet the User Responsibilities.

- Have all HMIS End Users sign a Verification of Receipt and Understanding related to this policy.
- Designate at least one Security Officer that has been trained to technologically uphold the Privacy Notice.

HMIS Lead Agency; System Administrator/Administration Responsibilities

HMIS Lead Agency has the responsibility to:

- Work with HMIS/CES Committee to create a Privacy Plan which meets or exceeds all minimum standards as described in the HUD Data and Technical Standards.
- Train and monitor all CHOs, End users, CHO staff and Security Officer upholding system privacy.
- Monitor CHOs to ensure adherence to the Privacy Plan.
- Maintain the CoC's HMIS webpage to keep all references within the Privacy Notice up to date.

Collecting PPI/PII

A provider must collect PPI/PII by lawful and fair means and, where appropriate, with the knowledge or consent of the individual. When a provider is required by law, or by a funding source to collect information it must ask for the required information, although participants may refuse to provide the information and still receive services. PPI/PII collected by CHOs may be required or may be collected to assist with monitoring project operations, to better understand the needs of people experiencing homelessness, and to improve services for people experiencing homelessness.

In all circumstances, providers should make data collection transparent by providing participants with a written copy of the CoC's Privacy Notice or informing clients where they can access the privacy notice, describing the notice in plain language, and posting a public statement in an easily visible manner.

Disclosures of PPI/PII

It might be necessary for a CHO to disclose client PPI/PII. Any disclosures must comply with HUD rules.

- "Uses" are internal activities for which providers interact with participant PII.
- "Disclosures" of PII occur when providers share PII with an external entity.

Data Disclosures Not Requiring Client Consent

Once collected, providers have obligations about how PPI/PII information may be used and disclosed. Uses and disclosures either are required by HUD (e.g., participants' access to their own information, oversight of compliance with the HMIS data privacy and security standards) or are permitted by HUD (e.g., to provide services, reporting to funders).

HUD's required and permitted uses and disclosures must be stated in the CoC's Privacy Notice. HUD requires two mandatory disclosures regardless of their inclusion in the Privacy Notice:

- Client access to their information; and
- Disclosures for oversight of compliance with HMIS privacy and security standards.

Permitted Disclosures

HUD permits the following uses and disclosures of PPI/PII without participant consent, provided that the uses and disclosures are listed in the CoC's Privacy Notice. If any of these uses and disclosures are not listed in the Privacy Notice, client consent is required:

- To provide or coordinate services to an individual;
- 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; and
- For creating de-identified datasets from PII.

HUD also permits the following types of uses and disclosures of PII without participant consent, provided that these additional uses and disclosures are listed in the Privacy Notice. If any of these uses and disclosures are not listed in the Privacy Notice, client consent is required:

- Uses and disclosures to avert a serious threat to health or safety;
- Uses and disclosures about victims of abuse, neglect or domestic violence; A CHO may disclose PPI/PII about an individual whom the CHO reasonably believes to be a victim of abuse, neglect or domestic violence to a government authority (including a social service or protective services agency) authorized by law to receive reports of abuse, neglect or domestic violence under any of the following circumstances:
    - Where the disclosure is required by law and the disclosure complies with and is limited to the requirements of the law;
    - If the individual agrees to the disclosure; or
    - To the extent that the disclosure is expressly authorized by statute or regulation; and
    - The CHO believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; OR if the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the PPI/PII for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

- A CHO that makes a permitted disclosure about victims of abuse, neglect or domestic violence must promptly inform the individual that a disclosure has been or will be made, except if:
    - The CHO, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or
    - The CHO would be informing a personal representative (such as a family member or friend), and the CHO reasonably believes the personal representative is responsible for the abuse, neglect or other injury, and that informing the personal representative would not be in the best interests of the individual as determined by the CHO, in the exercise of professional judgment.
- Uses and disclosures for research purposes;
- When a judge, administrative agency orders it; and
- Uses and disclosures for law enforcement purposes: A CHO may, consistent with applicable law and standards of ethical conduct, disclose PPI/PII for a law enforcement purpose to a law enforcement official **ONLY** under the following circumstances:
    - In response to a lawful court order, court-ordered warrant, subpoena or summons issued by a judicial officer, or a grand jury subpoena;
        - If the law enforcement official makes a written request for protected personal information that:
        - Is signed by a supervisory official of the law enforcement agency seeking the PPI/PII; **and**
        - States that the information is relevant and material to a legitimate law enforcement investigation; **and**
        - Identifies the PPI/PII sought; **and**
        - Is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; **and**
        - States that de-identified information could not be used to accomplish the purpose of the disclosure; **OR**
        - If the CHO believes in good faith that the PPI/PII constitutes evidence of criminal conduct that occurred on the premises of the CHO; **OR**
        - In response to a request for the purpose of identifying or locating a suspect, fugitive, material witness or missing person **and** the PPI/PII disclosed consists only of name, address, date of birth, place of birth, Social Security Number, and distinguishing physical characteristics; **OR**
        - If the official is an authorized federal official seeking PPI/PII for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a); or
        - For the conduct of investigations authorized by 18 U.S.C. 871 and 879

(threats against the President and others); **and**

- The information requested is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought.

If a CHO discloses information to law enforcement, the CHO must inform the HMIS Lead Agency within 24 hours of occurrence, and shall provide a written description of the circumstances, reason for disclosure and information disclosed. This can be submitted via email to HMISHelp@buttecounty.net

Required Disclosures

HUD requires two mandatory disclosures regardless of their inclusion in the Privacy Notice:

- Participants' access to their own information
- Disclosures for oversight of compliance with HMIS data privacy and security standards

Certain uses and disclosures may also be prohibited or otherwise restricted by other federal, state, or local laws. For instance, recipients of Violence Against Women Act (VAWA) funding are prohibited from disclosing PII without the participant's written consent.

Client Requests

Clients have the right to request in writing:

- A copy of all PPI/PII collected,
- An amendment to any PPI/PII used to make decisions about their care and services (this request may be denied at the discretion of the agency, but the client's request must be noted in the project records),
- An account of all disclosures of client PPI/PII,
- Restrictions on the type of information disclosed to outside partners,
- A current copy of the privacy notice.

CHOs may reserve the right to refuse a client's request for inspection or copies of PPI/PII in the following circumstances:

- Information compiled in reasonable anticipation of litigation or comparable proceedings,
- The record includes information about another individual (other than a health care or homeless provider),
- The information was obtained under a promise of confidentiality (other than a promise from a health care or homeless provider) and a disclosure would reveal the source of the information,

- The CHO believes that disclosure of the information would be reasonably likely to endanger the life or physical safety of any individual.

If a client submits a written request for the aforementioned information, CHO must respond in writing within five (5) business days. Additionally, CHO must only provide information related to PPI/PII collected by their agency. If a client is receiving services from multiple CHOs, the client must submit a written request to each agency.

If a client's request is denied, the CHO must be provided a written explanation of the reason of the denial. The client has the right to appeal the denial by following the established CHO grievance procedure, listed in the Privacy Notice. Regardless of the outcome of the appeal, the client shall have the right to add to his/her program records a concise statement of disagreement. The CHO shall disclose the statement of disagreement whenever it discloses the disputed PPI/PII.

If a CHO denies a client's request, they must submit the client's original written request as well as their written explanation of the denial to the HMIS Lead Agency within 24 hours of occurrence. This can be submitted via email to HMIShelp@buttecounty.net

Reporting Security Incidents

These Security Standards and the associated HMIS Policies and Procedures are intended to prevent, to the greatest degree possible, any security incidents. However, should a security incident occur, the following procedures should be followed in reporting:

- Any HMIS End User who becomes aware of or suspects a breach of HMIS system security and/or client privacy by another end user, they must immediately report that breach to the CHO Administrator. **Notification must occur within one (1) hour and in writing.**
- Any HMIS End User who becomes aware of or suspects a breach of HMIS system security and/or client privacy by the CHO or CHO Administrator, must immediately notify the HMIS Lead Agency. **Notification must occur within one (1) hour and be in writing.**
- In the event of a suspected security or privacy concern the CHO Security Officer should also immediately inform the HMIS Lead in writing, within one (1) hour (at HMIShelp@buttecounty.net) and conduct a complete an internal investigation.
    - If the suspected security or privacy concern resulted from an End User's suspected or demonstrated noncompliance with the HMIS End User Agreement, the HMIS Policy & Procedure, the HMIS Privacy and Security Plan, or the Privacy Notice, the CHO Security Officer must immediately and in writing request the HMIS Lead Agency deactivate the End User's User ID until the internal investigation has been completed.

- Following the internal investigation, the CHO Security Officer shall notify the HMIS Lead Agency of any substantiated incidents that may have compromised HMIS system security and/or client privacy whether or not a release of client PPI/PII is definitively known to have occurred. If the security or privacy concern resulted from demonstrated noncompliance by an End User with the HMIS End User Agreement, the HMIS Policy & Procedure, the HMIS Privacy and Security Plan, or the Privacy Notice, the HMIS Lead Agency will permanently deactivate the User ID for the End User in question.
- Within one (1) business day after the HMIS Lead Agency Security Officer receives notice of the security or privacy concern, the HMIS Lead Agency Security Officer and CHO Security Officer will jointly establish an action plan to analyze the source of the security or privacy concern and actively prevent such future concerns. The action plan shall be implemented as soon as possible, and the total term of the plan must not exceed thirty (30) days.
- If the CHO is not able to meet the terms of the action plan within the time allotted, the HMIS System Administrator, in consultation with the Butte Countywide Homeless Continuum of Care Executive Committee, may elect to terminate the CHO's access to HMIS. The CHO may appeal to the CoC Executive Committee for reinstatement to HMIS following completion of the requirements of the action plan.
- In the event of a substantiated release of PPI/PII in noncompliance with the provisions of these Security Standards, the Butte Countywide HMIS Policies and Procedures, or the Privacy Notice, the CHO Security Officer will make a reasonable attempt to notify all impacted individual(s) within seven (7) business days. The HMIS Lead Agency must approve of the method of notification and the CHO Security Officer must provide the HMIS Lead Agency Security Officer with evidence of the Agency's notification attempt(s). If the HMIS Lead Agency Security Officer is not satisfied with the Agency's efforts to notify impacted individuals, the HMIS Lead Agency Security Officer will attempt to notify impacted individuals at the CHO's expense.
- The HMIS Lead Agency will notify the appropriate body of the Continuum of Care of any substantiated release of PPI/PII in noncompliance with the provisions of these Security Standards, the HMIS Policies and Procedures, or the Privacy Notice within seven (7) business days.
- The HMIS Lead Agency will maintain a record for seven (7) years, of all substantiated releases of PPI/PII in noncompliance with the provisions of these Standards, the Butte Countywide County HMIS Policies and Procedures, or the Privacy Notice.
- The CoC reserves the right to permanently revoke a CHO's access to HMIS for substantiated noncompliance with the provisions of these Security Standards, the Butte Countywide HMIS Policies and Procedures, or the Privacy Notice if that noncompliance resulted in a substantiated release of PPI/PII.

System Security

Security Plan Overview

HMIS security standards are established to ensure the confidentiality and integrity of all HMIS information and data. The security standards are designed to protect against any reasonably anticipated threats or hazards to security and must be enforced by system administrators, CHO administrators as well as end users. This section is written to comply with section 4.3 of the 2004 Homeless Management Information Systems (HMIS) Data and Technical Standards Final Notice, as well as local legislation pertaining to maintaining an individual's personal information.

On December 9, 2011, HUD continued the process to implement the HEARTH Act, with the publication of the proposed rule titled "Homeless Management Information Systems Requirements" (76 FR 76917), which provides for uniform technical requirements for Homeless Management Information Systems (HMIS), for proper data collection and maintenance of the database, and ensures the confidentiality of the information in the database.

Meeting the minimum standards in this Security Plan is required for participation in the HMIS. Any agency may exceed the minimum standards described in this plan and are encouraged to do so. All CHO Administrators are responsible for understanding this policy and effectively communicating the Security Plan to individuals responsible for security at their agency.

Security Plan Applicability

The HMIS System and all CHOs must apply the security standards addressed in this Security Plan to all systems where PPI/PII is stored or accessed. Additionally, all security standards must be applied to all networked devices. This includes, but is not limited to, networks, desktops, laptops, tablets, mobile devices, mainframes and servers.

End Users are NOT allowed to use personal devices to access HMIS. Any End User found to be using a device not approved by and owned by CHO will immediately have their HMIS access removed and will receive a lifetime ban from the system.

All agencies, including the HMIS Lead, will be monitored by the HMIS System Administrators annually to ensure compliance with the Security Plan. Agencies that do not adhere to the security plan will be given thirty (30) calendar days, to address any concerns. Egregious violations of the security plan may result in immediate termination of a CHO or user's access to HMIS as determined by the HMIS Lead.

Security Officers

The HMIS Lead Agency and all HMIS Partner Agencies must designate Security Officers to oversee HMIS privacy and security. A single point-of-contact who is responsible for annually certifying that Agencies adhere to the Security Plan; testing the CoC's security practices for compliance. As of the writing of this plan, HMIS Lead Agency's Security Officer and the HMIS

Lead are the same person.

HMIS Lead Agency 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; and
- Assesses security measures in place prior to establishing access to HMIS for a new CHO; and
- Reviews and maintains file of CHO "HMIS Quarterly Compliance Certification Checklist"; and
- Conducts annual security audit of all CHOs.

CHO Security Officer

- May be the CHOs HMIS Administrator or another employee, volunteer or contractor who has completed HMIS Privacy and Security training and is adequately skilled to assess HMIS security compliance; and
- Conducts a security audit for all workstation that will be used for HMIS purposes;
    - No less than quarterly for all agency HMIS workstations, and devices; and
    - Prior to requesting a User ID to a new HMIS End User; and
    - Any time an existing user moves to a new workstation.
- Continually ensures each workstation within the CHO used for HMIS data collection or entry is adequately protected by a firewall and antivirus software (see Technical Safeguards – Workstation Security); and
- Completes the "HMIS Quarterly Compliance Certification Checklist", and forwards the Checklist to the HMIS Lead Agency Security Officer via email sent to HMISHelp@buttecounty.net

Physical Safeguards

In order to protect client privacy, it is important that the following physical safeguards be put in place. For the purpose of this section, authorized persons will be considered only those individuals who have completed Privacy and Security training within the past 12 months.

- Computer Location – A computer used as an HMIS workstation must be in a secure location where only authorized persons have access. The workstation must not be accessible to clients, the public or other unauthorized CHO staff members or volunteers. A password protected automatic screen saver will be enabled on any computer used for HMIS data entry. The screensaver must be set at no more than fifteen (15) minutes.
- Printer location – Documents printed from HMIS must be sent to a printer in a secure

location where only authorized persons have access.

- Computer Access (visual) — Non-authorized persons should not be able to see an HMIS workstation screen. Monitors should be turned away from the public or other unauthorized CHO staff members or volunteers and utilize visibility filters to protect client privacy.
- Mobile Device – A mobile device used to access and enter information into the HMIS system must use a password or other user authentication on the lock screen to prevent an unauthorized user from accessing it and it should be set to automatically lock after no more than five (5) minutes of device inactivity. A remote wipe and/or remote disable option should also be downloaded onto the device.
- CHO approved devices – CHO staff and HMIS End Users must only use devices purchased, approved and secured by the CHO for access to HMIS. If a CHO administrator finds an End User has accessed HMIS on a non-authorized device, either a personal device or on an agency purchased device while not "on the clock", the CHO Administrator must inform the HMIS Lead Agency within one (1) hour, the End User will immediately and permanently lose access to HMIS.

Technical Safeguards

Workstation Security

- To promote the security of HMIS and the confidentiality of the data contained therein, access to HMIS will be available only through approved workstations; and
- The HMIS Lead Agency will enlist the use of an IP Address Whitelist or another suitably secure method to identify approved workstations, in compliance with Public Access baseline requirement in the HUD Data Standards (4.3.1 System Security). CHOs may be required to submit the IP Address of their workstation to the HMIS Lead Agency to be registered into the system and will notify the Lead Agency should this number need to be changed; and
- CHO Security Officer will confirm that any workstation accessing HMIS shall have antivirus software with current virus definitions (updated at minimum every 24 hours) and frequent full system scans (at minimum weekly); and
- CHO Security Officer will confirm that any workstation accessing HMIS has and uses a hardware or software firewall; either on the workstation itself if it accesses the internet through a modem or on the central server if the workstation(s) accesses the internet through the server.

Establishing HMIS User IDs and Access Levels

- The CHO Administrator, will ensure that any prospective End User reads and understands the HMIS End User Agreement prior to training.
- Upon logging into HMIS for the first time, and every six (6) months thereafter, HMIS End

Users will be prompted to read and sign the End User Agreement. The HMIS System will maintain a file of all signed HMIS End User Agreements.

- The CHO Administrator, in conjunction with the HMIS Lead is responsible for ensuring that all End Users have completed mandatory trainings, including but not limited to HMIS Privacy, Security and Ethics training, and End User Responsibilities, prior to being provided with a User ID to access HMIS. Currently, training is included as a part of the new user HMIS training.
- All End Users will be issued a unique User ID and password. Sharing of User IDs and passwords is expressly prohibited. Each End User must be specifically identified as the sole holder of a User ID and password. User IDs and passwords may not be transferred from one user to another.
- The HMIS System Administrator will always attempt to assign the most restrictive access that allows an End User to efficiently and effectively perform his/her duties.
- The HMIS System Administrator will create the new User ID and notify the User ID owner of the temporary password.
- When the CHO determines that it is necessary to change a user's access level, the HMIS System Administrator will update the user's access level as needed.

User Authentication

- User IDs are individual and passwords are confidential. No individual should ever use or allow use of a User ID that is not assigned to that individual, and user- specified passwords should never be shared or communicated in any format.
- Temporary passwords must be changed on first use. User-specified passwords must be a minimum of 6 characters long and must contain a combination of upper case and lower-case letters, a number and a symbol.
- End users will be prompted by the software to change their password every 90 days.
- End Users must immediately notify the HMIS System Administrator if they have reason to believe that someone else has gained access to their password.
- Three consecutive unsuccessful attempts to login will disable the User ID until the password is reset. For End Users, passwords must be reset by the HMIS System Administrator.
- Users must log out from the HMIS application and either lock or log off their respective workstation if they leave. If the user logged into HMIS and the period of inactivity in HMIS exceeds 45minutes, the user will be logged off the HMIS system automatically.

Rescinding User Access

- The CHO Administrator will notify the HMIS System Administrator within 24-hours if an

End User no longer requires access to perform his or her assigned duties due to a change of job duties or termination of employment.

- The HMIS System Administrator reserves the right to terminate End User licenses that are inactive for 45 days or more. The HMIS System Administrator will attempt to contact the CHO for the End User in question prior to termination of the user's license.
- In the event of suspected or demonstrated noncompliance by an End User with the HMIS End User Agreement or any other HMIS plans, forms, standards or governance documents, the CHO Administrator or CHO Security Officer shall notify the HMIS System Administrator to deactivate the User ID for the End User in question until an internal agency investigation has been completed. The HMIS Lead Agency should be notified of any incidents that may have resulted in a breach of HMIS system security and/or client confidentiality, whether or not a breach is definitively known to have occurred.
- Any agency personnel who are found to have misappropriated client data (identity theft, releasing personal client data to any unauthorized party), shall have HMIS privileges revoked and may be subject to criminal prosecution under any relevant federal or state laws.
- The CoC is empowered to permanently revoke a CHO or an End User's access to HMIS for substantiated noncompliance with the provisions of these Security Standards, the Butte Countywide CoC's HMIS Policies and Procedures, the Butte Countywide CoC's CES Policies and Procedures, or the HMIS Privacy Notice that resulted in a release of PPI/PII.

Disposing Electronic, Hardcopies, Etc.

- All technology equipment including but not limited to computers, mobile devices, tablets, printers, copiers and fax machines used to access HMIS and which will no longer be used to access HMIS must have their hard drives reformatted multiple times. If the device is now non-functional, it must have the hard drive pulled, destroyed and disposed of in a secure fashion. If the device does not have a hard drive CHOs must use software tools that will thoroughly delete/wipe all information on the device and return it to the original factory state before discarding or reusing the device.
- Hardcopies: For paper records, shredding, burning, pulping, or pulverizing the records so that PPI/PII is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed.
- The HMIS Lead Agency shall develop and implement procedures for managing new, retired, and compromised HMIS account credentials.
- The CHO Administrator in conjunction with the CHO Security Officer shall develop and implement procedures for managing new, retired, and compromised local system account credentials.
- The CHO Security Officer shall develop and implement procedures that will prevent unauthorized users from connecting to private agency networks.
- Unencrypted PPI/PII may not be stored or transmitted in any fashion—including sending

file attachments by email or downloading reports including PPI/PII to a flash drive, to the End User's desktop or to an agency shared drive. All downloaded files containing PPI/PII must be deleted from the workstation temporary files and the "Recycling Bin" emptied before the End User leaves the workstation.

Disaster Recovery Plan

Disaster recovery for the Butte Countywide Continuum of Care HMIS will be conducted by the HMIS System Administrator with support from the HMIS software vendor as needed. The HMIS System Administrator must be familiar with the disaster recovery plan set in place by the HMIS software vendor.

- The HMIS System Administrator should maintain ready access to the following information:
    - Contact information – Phone number and email address of the software vendor contact person responsible for recovering the Continuum of Care's data after a disaster.
    - HMIS System Administrator responsibilities – A thorough understanding of the HMIS System Administrator's role in facilitating recovery from a disaster.
- All HMIS System Administrators should be aware of and trained to complete any tasks or procedures for which they are responsible in the event of a disaster.
- The HMIS System Administrator must have a plan for restoring local computing capabilities and internet connectivity for the HMIS System Administrator's facilities.

This plan should include the following provisions.

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

Workforce Security

HMIS Access to Active Clients

The Butte Countywide Homeless CoC operates a shared HMIS system, allowing HMIS Users to access client records from various agencies. To maintain the security and integrity of the HMIS and safeguard the confidentiality of personal information, the following policy is in effect:

Effective immediately, the HMIS Lead Agency will no longer grant HMIS End Users access to the records of individuals who are actively receiving services from the CHO agency that employs them.

If an HMIS End User is currently receiving services from another CHO agency, the user or prospective user must promptly notify that agency of their current or upcoming HMIS work role. The CHO agency providing services will designate an HMIS End User, preferably the CHO Administrator, to manage the cases and services of any active HMIS Users.

Additionally, the CHO agency must create a new, privatized client profile for the HMIS User receiving services to ensure the individual cannot access their own file within the system. All services and programs must be provided and tracked within this new privatized profile. The CHO agency is also responsible for informing the HMIS Lead Agency that they are providing services for an active or prospective HMIS User. The HMIS Lead Agency will then periodically audit the case to ensure that only authorized staff members are accessing the client's case. Any unauthorized access to the case may result in the loss of HMIS access for the offending party due to a violation of client privacy rules.

Background Check

HMIS User Background Check Requirements

The Butte CoC recognizes the sensitivity of the data in HMIS, and therefore requires individuals responsible for managing, entering and/or accessing HMIS data be subject to a criminal background check.

No prospective end user or CHO HMIS Administrator will be given HMIS access if he, she or they have entered a plea of nolo contendere (no contest) or has been found guilty of any misdemeanor or felony fraud (including but not limited to) identity theft, stalking, human trafficking or any related crimes. HMIS Participating Agencies cannot risk the privacy and confidentiality of client information by allowing HMIS access to any individual who pled nolo contendere or been found guilty of the aforementioned crimes. In the broadest sense, a fraud is an intentional deception made for personal gain or to damage another individual. HMIS participating agencies are solely responsible for conducting background checks on their employees or contract workers, who will be accessing HMIS, and are responsible for any associated costs.

The background check must include local and state records; agencies are strongly encouraged to include federal records as well. Background checks must be run in accordance with state law. Background timelines should include the last 7 years. Background checks that come back with a criminal history should be carefully considered prior to giving an employee access to client information. If a HMIS participating agency is unsure if a prospective HMIS End User's criminal history could or should preclude them from accessing HMIS, they must contact the CoC's
HMIS Lead to determine eligibility prior to submitting a request to grant the End User access.
A background check may be conducted only once for each person unless otherwise required, and the results of the background check must be retained in the employee's personnel file through the term of their employment. All End Users must have a completed background check prior to access being requested to HMIS by a CHO. Criminal background checks must be completed on all new End Users and CHO HMIS Administrators, and the "Background Check Review and Verification Statement" must be signed by the Agency's Director, the CHO HMIS Administrator, or the Head of the HR Department.

CHO Procedure

Agencies must have a policy regarding conducting background checks and hiring individuals

with criminal justice histories consistent with HMIS Privacy and Security Plan. HMIS Participating Agencies should not risk the privacy and confidentiality of client information by allowing any individual convicted of fraud or a stalking related crime in any state. In the broadest sense, a fraud is an intentional deception made for personal gain or to damage another individual.

- Background checks that come back with a criminal history should be carefully considered prior to giving an employee access to client information.
- All End Users should have had a background check prior to access being requested to the HMIS by a CHO.
- Criminal background checks must be completed on all new End Users, and the "Background Check Template" must be completed on agency letterhead and signed by the HR Department or the agency's Executive Director. Additionally, it must be submitted to the HMIS Lead Agency prior to End Users gaining access to the HMIS.

HMIS Lead Procedure

The HMIS Lead Agency Security Officer and all Administrators must also undergo criminal background verification. The HMIS Lead will hire individuals with criminal justice histories only to the extent the hire is consistent with any relevant hiring policies of the Lead Agency, unless the background check reveals a history of crimes related to identity theft or fraud.

List of crimes considered to fall in this category

A staff member's background check revealing a history of following crimes related to identity theft or fraud will not be given access to the HMIS. The CHO's HR Department or Executive Director must only sign the Background Check Review and Verification Statement if staff's background check doesn't reveal a history of following have entered a plea of nolo contendere (no contest) or has been found guilty of any misdemeanor or felony fraud, including but not limited to, identity theft, stalking, human trafficking or any related crimes:

- **Bank Fraud:** To engage in an act or pattern of activity where the purpose is to defraud a bank of funds.
- **Blackmail:** A demand for money or other consideration under threat to do bodily harm, to injure property, to accuse of a crime, or to expose secrets.
- **Bribery:** When money, goods, services, information or anything else of value is offered with intent to influence the actions, opinions, or decisions of the taker. You may be charged with bribery whether you offer the bribe or accept it.
- **Computer fraud:** Where computer hackers steal information sources contained on computers such as: bank information, credit cards, and proprietary information.
- **Credit Card Fraud:** The unauthorized use of a credit card to obtain goods of value.
- **Extortion:** Occurs when one person illegally obtains property from another by actual or

threatened force, fear, or violence, or under cover of official right.

- **Forgery:** When a person passes a false or worthless instrument such as a check or counterfeit security with the intent to defraud or injure the recipient.
- **Health Care Fraud:** Where an unlicensed health care provider provides services under the guise of being licensed and obtains monetary benefit for the service.
- **Larceny/Theft:** When a person wrongfully takes another person's money or property with the intent to appropriate, convert or steal it.
- **Money Laundering:** The investment or transfer of money from racketeering, drug transactions or other embezzlement schemes so that it appears that its original source either cannot be traced or is legitimate.
- **Telemarketing Fraud:** Actors operate out of boiler rooms and place telephone calls to residences and corporations where the actor requests a donation to an alleged charitable organization or where the actor requests money up front or a credit card number up front, and does not use the donation for the stated purpose.
- **Welfare Fraud:** To engage in an act or acts where the purpose is to obtain benefits (i.e. Public Assistance, Food Stamps, or Medicaid) from the State or Federal Government.

Privacy and Security Monitoring

New HMIS CHO Site Security Assessment

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

Quarterly CHO Self-Audits

- The CHO Security Officer will use the "HMIS Quarterly Compliance Checklist "to conduct quarterly security audits of all CHO HMIS End User workstations.
- The CHO Security Officer will audit for inappropriate remote access by End-Users by associating User login date/times with employee time sheets. End Users must certify that they will not remotely access HMIS from a workstation (ie: personal computer, phone, tablet or any other device) that is not subject to the CHO Security Officer's regular audits.
- If areas are identified that require action due to noncompliance with these standards or any element of the Butte Countywide HMIS Policies and Procedures, the CHO Security

Officer will note these on the Checklist, and the CHO Security Officer in conjunction with the CHO Administrator will work to resolve the action item(s) within 15 calendar days.

- Any "HMIS Quarterly Compliance Checklist" that includes 1 or more findings of noncompliance and/or action items will not be considered complete until all action items have been resolved. The findings, action items, and resolution summary must be reviewed and signed by the CHO's Executive Director or other empowered officer prior to being forwarded to the HMIS Lead Agency Security Officer.
- The CHO Security Officer must turn in a copy of the "HMIS Quarterly Compliance Checklist" to the HMIS Lead Agency Security Officer on a quarterly basis. This can be turned in via email by sending a signed copy to HMIShelp@buttecounty.net
- The CHO will retain in their records the original signed copy of the "HMIS Quarterly Compliance Checklist" for a minimum of seven (7) years.

Annual Security Audits

- The HMIS Lead Agency Security Officer will schedule the annual security audit a minimum of thirty (30) calendar days in advance with the CHO Security Officer.
- The HMIS Lead Agency Security Officer will use both the "HMIS Quarterly Compliance Checklist" and the "HMIS Lead Privacy & Security Compliance Checklist" to conduct security audits.
- The HMIS Lead Agency Security Officer must randomly audit at a minimum 10% of the workstations used for HMIS data entry for each HMIS CHO project site. In the event that an agency has more than one (1) project site, all project sites must be audited.
- If areas are identified that require action due to noncompliance with these standards or any element of the Butte Countywide HMIS Policies and Procedures, or the Privacy Notice, the HMIS Lead Agency Security Officer will note these on the Checklist, and the CHO Security Officer and/or HMIS Agency Administrator will work to resolve the action item(s) within fifteen calendar (15) days.
- Any Checklist that includes one (1) or more findings of noncompliance and/or action items will not be considered complete until all action items have been resolved and the findings, action items, and resolution summary has been reviewed and signed by the CHO's Executive Director or other empowered officer and forwarded to the HMIS Lead Agency Security Officer.

Client Approved Authorized Representative

An Authorized Representative (AR) is an individual appointed by a customer to accompany, assist and represent them in their application for services. An AR may also access the customer's Personal Protected Information (PPI) and their Personal Identifying Information (PII). An Authorized Representative can be family members, friends, or any other individual chosen by the client.

Some clients may request an Authorized Representative who can assist them when applying for services, enrolling in a program, or in updating their information in HMIS. If a client requests an AR, CHO staff must complete a "HMIS Authorized Representative (AR) Form". This form can be found in the Appendix.

When completing the form, CHO staff must:

- Ensure all parties signing the form are physically present (client, AR, and CHO staff); and
- All portions of the form are completed Incomplete forms will not be accepted); and
- The client understands the two levels of authorization, and they choose only one option; and
- All parties are provided a copy of the form; and
- Immediately upload the completed form to the client level files; and
    - File Category "Authorized Representative HMIS"
    - File Name "Authorized Representative (initial form)"
- Immediately enter a detailed client level note regarding the meeting with the client and AR; and
- Immediately updated the client's profile page with the AR's information.

Clients can revoke AR authorization at any time, without the AR's knowledge or consent. Should a client revoke an AR's authorization CHO staff must:

- Download the original authorization form from HMIS; and
- Have the client initial in the revocation section of the form; and
- Provide the client with a copy of the updated form; and
- Immediately upload the initialed form to the client level files; and
    - File Category "Authorized Representative HMIS"
    - File Name "Authorized Representative (Revocation Form)"
- Immediately **delete** the AR's information from the client's profile page; and
    - Deactivate the slider indicating the client has an AR.
- Immediately enter a detailed client level note regarding the revocation of the AR.

CoC Approved Public Notice

HUD requires the posting of a Public Notice at all workstations in which HMIS data is collected and/or entered into the system where clients are present. This includes when CHO staff are conducting outreach and engagement in the community.

The Public Notice must be easily visible to clients. The presence of the Public Notice informs clients that their information is being collected and stored in HMIS. The notice also informs client they can review the CoC's full privacy notice for more details if they request it.

It is not necessary to discuss notice with client unless they request more information. However, if a client requests more information, do discuss it and provide the client with the CoC's Privacy Notice.

BUTTE COUNTYWIDE CONTINUUM OF CARE'S HMIS PUBLIC NOTICE

We collect personal information directly from you for our local Homeless Management Information System (HMIS). We may be required to collect personal information by law or by organizations that give us money to operate this program.

The collection and use of all personal information are guided by strict standards of confidentiality. The only people allowed to see the information we collect are local homeless service providers who are committed to assisting you and keeping your information confidential.

The personal information we collect is important to run our programs, to improve services for persons experiencing homelessness, and to better understand the needs of persons experiencing homelessness. We only collect information we are required to, and consider to be appropriate.

CoC Approved Privacy Notice

The notice is attached to this plan and can be found in Appendix A.

Definitions

Uses in relation to PPI/PII are internal activities for which providers interact with participant PII.

Disclosures in relation to PPI/PII occur when providers share PII with an external entity.

Authorized Representative (AR) – an individual appointed by a customer to accompany, assist and represent them in their application for services. An AR may also access the customer's Personal Protected Information (PPI) and their Personal Identifying Information (PII). An Authorized Representative can be family members, friends, or any other individual chosen by the client.

Annual Homeless Assessment Report (AHAR) HUD's annual report to Congress on the nature and extent of homelessness nationwide.

Annual Performance Report (APR) A reporting tool that HUD uses to track program progress and accomplishments of HUD homeless assistance programs on an annual basis (Formerly known as the Annual Progress Report).

Client A living individual about whom a Contributing HMIS Organization (CHO) collects or maintains protected personal information (1) because the individual is receiving, has received, may receive, or has inquired about services from CHO or (2) in order to identify services, needs, or to plan or develop appropriate services within the CoC.

Contributing HMIS Organization (or CHO) Any organization (employees, volunteers, and contractors) that records, uses or processes Protected Personal Information. This is what we commonly refer to within HMIS as an Agency and includes all associated staff.

Continuum of Care (CoC) means 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.

Data Recipient A person who obtains PPI/PII from an HMIS Lead Agency or from a CHO for research or other purpose not directly related to the operation of the HMIS, CoC, HMIS Lead Agency, or CHO.

Homeless Management Information System (HMIS) means the information system designated by Continuums of Care to comply with the requirements of HUD 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.

HMIS Lead Agency means an entity designated by the Continuum of Care in accordance with HUD to operate the Continuum's HMIS on its behalf.

HMIS Software Solution Provider An organization that sells, licenses, donates, builds or otherwise supplies the HMIS user interface, application functionality and database.

HMIS Participating Bed For any residential homeless program, a bed is considered a "participating HMIS bed" if the program makes a reasonable effort to record all universal data elements on all clients served in that bed and discloses that information through agreed upon means to the HMIS Lead Agency at least once annually.

HMIS vendor means 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.
HUD means the Department of Housing and Urban Development.

HMIS Committee is a group composed of representatives from interested CHOs who assist in making decisions regarding the HMIS system, HMIS policies and procedures, and any concerns that arise regarding it.

HMIS Participation Agreement is a written agreement between the HMIS Lead Agency and each CHO that details responsibilities of each party regarding participation in the COC HMIS.

Privacy is the control over the extent, timing, and circumstances of sharing oneself (physically, behaviorally, or intellectually) with others. Privacy consists of ensuring specific measures are in place when dealing with personal information and includes directives on when it is collected, how that information is used and how that information is shared with others.

Privacy Standards apply to all Agencies and Programs that record, use or process Protected Personal Information (PPI/PII) within the HMIS, regardless of funding source.

Protected Identifying Information or Personal Identifying Information (PPI/PII) means any information about a client that (1) identifies a specific individual, (2) can be manipulated so that identification is possible, (3) can be linked with other available information to identify a specific individual. This can include: name, SSN, program Entry/Exit, zip code of last permanent address, system/program ID, and program type.

Research A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to general knowledge.

Unduplicated Accounting of Homelessness An unduplicated accounting of homelessness includes measuring the extent and nature of homelessness (including an unduplicated count of homeless persons), utilization of homelessness programs over time, and the effectiveness of homelessness programs.

Unduplicated Count of Homeless Persons An enumeration of homeless persons where each person is counted only once during a defined period of time.

Victim service provider means 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 programs, and other programs.

Appendices of Forms

- Appendix A; HMIS Privacy Notice
- Appendix B; HMIS Public Notice
- Appendix C; End User Agreement
- Appendix D; HMIS Informed Consent
- Appendix E; Privacy Notice Quick Guide for Organizations in the Butte Countywide Homeless Continuum of Care
- Appendix F; Acknowledgement of Receipt
- Appendix G; Quarterly Compliance Checklist
- Appendix H; HMIS Lead Privacy & Security Compliance Checklist
- Appendix I; Background Check Template
- Appendix J; Authorized Representative

Resources

2004 HUD HMIS Data and Technical Standards, U.S. Dept. of Housing and Urban Development
https://www.hudexchange.info/resource/1318/2004-hmis-data-and-technical-standards-final-notice/

2024 HMIS Data Standards, U.S. Dept. of Housing and Urban Development
https://files.hudexchange.info/resources/documents/HMIS-Data-Standards-Manual-2024.pdf

2024 HMIS Data Dictionary, U.S. Dept. of Housing and Urban Development
https://files.hudexchange.info/resources/documents/HMIS-Data-Dictionary-2024.pdf

Document Revision History

Date	Version	Editor/Author	Notes
7/23/24	1.0	Elisa Rawlinson	Initial Draft – New Version of Policies & Procedures
	1.0	HMIS/CES Committee	Approved by HMIS/CES Committee
	1.0	CoC	Approved by the CoC

Appendix A; HMIS Privacy Notice

Butte Countywide Homeless Continuum of Care (CoC)
Homeless Management Information System (HMIS) Privacy Notice

PURPOSE

This Privacy Notice applies to all Butte Countywide Homeless Continuum of Care HMIS-Participating Agencies (Agencies) and their employees. This notice addresses how information about you (client) shall be used and disclosed by Agencies as well as rights over your information. This notice establishes minimum standards by which the Agencies must follow. Agencies may implement more stringent rules and procedures. We encourage you to read it in full.

We may use or disclose your information to provide you with services, and to comply with legal and other obligations. We assume that, by requesting services from an HMIS participating agency, you agree to allow them to collect information and to use or disclose it as described in this notice and as otherwise required by law. If you have any questions about this Privacy Notice, you may contact either your service provider, or the Butte Countywide Continuum of Care at; 205 Mira Loma Drive, Suite 50, Oroville, CA 95965, (530) 552-6200, HMIShelp@buttecounty.net

CHANGES TO THIS NOTICE

We reserve the right to revise or amend the terms of this Privacy Notice, and to retroactively apply any changes to our policies and procedures regarding your information. This notice is not a legal contract. If this notice is amended, a copy of the revised notice will be available upon request and posted on HMIS Participating agency websites.

WE ARE LEGALLY REQUIRED TO

Keep your information confidential, upon request provide you a copy of this notice of our legal duties and privacy practices with respect to your information, and to comply with this notice.

WHY WE COLLECT YOUR INFORMATION

A Homeless Management Information System (HMIS) is a local information technology system used to collect data on housing and services provided to persons experiencing or at risk of homelessness. This information is critical to better understand the extent and nature of homelessness at a local level, evaluate program effectiveness, and improve future housing and service provision. We also use HMIS to provide and coordinate services you receive, and to carry out administrative functions related to those services, such as payment or reimbursement for services. We produce statistical information related to those who access services and report this information through various means.

We collect information about the persons we serve in the shared HMIS (HMIS) database. The agency shall only collect information deemed appropriate and necessary for program operation or information that is required by law or by the organizations that fund this program.

Our community uses Clarity (the local HMIS software) to keep computerized case records. The information we collect and share includes: basic identifying demographic data such as name, date of birth, age, gender,

race, ethnicity, veteran status, and partial SSN ("Standard Information"); the nature of your situation, enrollment and assessment information, and the services and referrals you receive from this agency. This information is known as your Protected Personal Information (PPI).

Information is shared amongst Agencies, with the exception of Protected Service Providers. These protected agencies serve specific client populations, such as domestic abuse, sexual abuse, HIV/AIDS, alcohol and/or substance abuse, and mental health, and do not share client information about those issues.

BENEFITS OF INFORMATION COLLECTION AND SHARING

Information provided by you plays an important role in the ability of the CoC and local homeless service providers to continue providing the programs, services, and referrals that are appropriate for you. Information shared with other agencies also helps us develop new and more efficient programs. This allows us to:

1. Better demonstrate the need for services and the specific types of assistance needed in our community.
2. Make appropriate services available to meet community needs.
3. Plan, improve, and deliver quality services.
4. Keep required statistics for state and federal funders, like HUD.

CONSENT

You have the right to indicate that you do not want your Standard Information to be shared. In general, services will not be denied should you choose not to share your information. Written consent to share your data in HMIS should be obtained at your first in-person meeting with an HMIS Participating Agency.

Verbal consent to share your PII may only be obtained if the interaction meets the following criteria:

- The visit is not in person or not in a place conducive to paper signature.
- Agency staff read and complete the Informed Consent indicating the client gave verbal consent.

Other uses and disclosures of your information not covered by this Notice or the laws that apply will be made only with your written authorization. If you provide us authorization to disclose your information, you may revoke that authorization, in writing, at any time. If you revoke your authorization, we will no longer use or disclose your information for the reasons covered by the authorization, except, we are unable to take back any disclosures we have already made when the authorization was in effect, and we are required to retain our records of the services that we provided to you.

CONFIDENTIALITY RIGHTS

Every person and agency that is authorized to read or enter information into HMIS has been trained on client confidentiality policies and has signed an agreement to maintain the security and confidentiality of the information. Any person or agency that is found to violate their agreement may have their access rights terminated and may be subject to further State and federal legal and/or criminal penalties and liabilities.

PERMITED USES AND DISCLOSURES

HMIS is designed to protect the confidentiality of personal information while allowing for reasonable, responsible, and limited uses and disclosures of data, including PPI/PII once collected, we have obligations regarding how data may be used and disclosed (**uses** are internal activities for which providers interact with your PPI/PII; **disclosures** occur when providers share PPI/PII with an external entity). **We may use and disclose your PPI/PII only for the following purposes:**

(1) To allow you to access to your information; and

(2) To provide or coordinate services to an individual or household;

(3) Disclosures for oversight of compliance with HMIS privacy and security standards.

(4) For functions related to payment or reimbursement for services;

(5) To carry out administrative functions, including but not limited to legal, audit, personnel, oversight and management functions;

(6) For creating de-identified reporting from PII;

Service Collaboration: We understand telling your story to every agency you work with can be traumatizing. Therefore, may use and disclose your information so you do not have to provide information (tell your story) more than once. This can also help avoid duplication of services and referrals that you are already receiving.

Housing: We create a record of your information, including any housing services you receive from our partner agencies. Participating agencies may use or disclose your information to other personnel who are involved in providing services for you. For example, a housing navigator may need to know disability information to provide appropriate housing resources. Your service team may also share your information in order to coordinate the different things you need, such as referrals and services.

Participating agencies may use and disclose your information to other participating HMIS agencies as allow by law. We also may use and disclose your information in order to recommend service options or alternatives that may be of interest to you or assist you in obtaining and maintaining housing. Additionally, we may use and disclose your information to tell you about, and connect you to health-related benefits or services that may be of assistance to you. For example, Medi-Cal eligibility or Social Security benefits. You have the right to refuse this information.

USES AND DISCLOSURES THAT DO NOT REQUIRE YOUR AUTHORIZATION

We may use or disclose your PPI/PII for other reasons, even without your permission. Subject to applicable federal or state law, we are permitted to disclose your PPI/PII without your permission for the following purposes:

Research: Under certain circumstances, we may use and disclose information about you for research purposes. For example, a research project may involve comparing local services provided to the services of other communities. Before the use or disclosure of information for research purposes the project, is subject to a special approval process. This process evaluates the proposed research project and its use of information, while balancing the research needs with clients' need for privacy of their information.
Additionally, only aggregate or de-identified information about you may be disclosed to people conducting research.

As Required by Law: We will use and disclose information when required by federal or state law or regulation.
To Avert a Serious Threat to Health or Safety: We may use and disclose your information when necessary to prevent a serious threat to your health and safety or the health and safety of the public or another person.

Public Health Activities: We may disclose your information for public health activities such as to report the abuse or neglect of children, elders, and dependent adults.

Law Enforcement: We may disclose your information to law enforcement under the following circumstances:

- In response to a Court order, warrant, subpoena, summons or similar legal process;
- About a death we believe may be the result of criminal conduct;
- About criminal conduct at any of our facilities;
- In emergency circumstances; or
- In cases of Abuse, Neglect, or Domestic Violence.
    - If we believe you have been the victim of abuse, neglect, or domestic violence. We will only make this disclosure if you agree or when required or authorized by law.

Oversight Activities: We may disclose your information to an oversight agency, such as the Department of Housing and Urban Development (HUD) or the State of California, for activities authorized by or required by law. These oversight activities are necessary to monitor service programs, and to comply with civil rights laws.

HMIS Providers must also ensure that **any use or disclosure does not violate other applicable local, state, or federal laws**. Therefore, some HMIS Providers **may have more restrictive privacy policies**, often dependent upon funding source or the nature of a project. Specific, per-project information regarding data use and disclosure can be obtained upon request. This can include agencies that must comply with the Health Insurance Portability and Accountability Act (HIPAA), Violence Against Women Act (VAWA). In these instances, the more restrictive policies take precedence.

In addition, the company that provides our local HMIS may access PPI, for the purposed of aggregating PPI with the data of other individuals stored in HMIS for the creation and maintenance of client records.

When we prepare reports and statistical information or disclose information from HMIS to other parties for research or evaluation purposes, we de-identify the information before we disclose it. “De-identifying” information refers to the process in which all personal protected information (PPI) and personal identifying information (PII) are removed from data so information related to programs and services cannot be used directly or indirectly to identify you or any other individual.

Maintaining the privacy and safety of persons accessing our services is of the utmost importance to us. We believe information gathered from you is personal and private. We collect information only when appropriate to provide services, manage our organization, or as required by law.

YOUR RIGHTS REGARDING INFORMATION ABOUT YOU

The CoC recognizes every independent legal adult (person age 18 and up) as the owner of all information about themselves, and any parent, legal guardian, or legal power of attorney as the designated owner of all information about any household members under their guardianship (all

minors and any incapacitated/disabled adults).

By seeking assistance from this HMIS Provider and consenting to your personal information being shared within the HMIS, you transfer governance responsibility ~~of~~ your HMIS record to us. We are responsible for handling your record in accordance with HMIS privacy policies and any applicable federal, state, or local requirements. You retain ownership of your information within your HMIS record, and as owner you have the following rights, in general:

- You have the right to see your information, request to change it, and have a copy of your information from the servicing agency by written request. You may also request assistance from this agency in documenting your history of homelessness to qualify for certain programs. An agency can refuse to change information but must provide you with a written explanation of the refusal within five (5) days of the request.
- Any information you provide related to race, color, religion, sex, national origin, disability, familial status, and actual or perceived sexual orientation, gender identity, or marital status will not be used in any way that would discriminate against you or prevent you from receiving services or housing assistance. You have the right to file a complaint if you feel that you have been discriminated against.
- You may request that a provider mark your personal data as private (not shared) within HMIS.
- You may withdraw your consent to share at any time in writing. However, any information already shared with another agency cannot be taken back. Your request to discontinue sharing will have to be coordinated between sharing partners. You must inform each agency you work with when you withdraw your consent.
- The confidentiality of your records is protected by law. This agency will never give information about you to anyone outside the agency without your specific written consent through this release or as required by law (The regulations are the Federal Law of Confidentiality for Alcohol and Drug Abuse Patients, (42 CFR, Part 2) and the Health Insurance Portability and Accountability Act of 1996 (HIPPA), 45 CRF, Parts 160 & 164) and applicable California laws.

You should expect to provide additional, prior written consent for any use or disclosure of HMIS PII not included in the permitted uses and disclosures above.

Right to Inspect and Obtain Copies and to Request an Amendment: With certain exceptions, you have the right to review and obtain copies of your HMIS record or request your record be amended. You must submit a request, in writing, to the service provider where you received services. Your request will become a part of your record. We will respond to your request within five (5) business days.

Agency's Right to Refuse Inspection of an Individual Record: The CoC and service providers may deny your request to inspect, copy, or amend your PPI/PII, and must document those reasons in their response to your request. Reasons can include:

(1) The information is compiled in reasonable anticipation of litigation or comparable proceedings;
(2) Information about another individual, other than our staff, would be disclosed;
(3) Information was obtained under a promise of confidentiality other than a promise from this provider and disclosure would reveal the source of the information; or

(4) The disclosure of information would be reasonably likely to endanger the life or physical safety of any individual.
(5) Harassment. We reserve the right to reject repeated or harassing requests for access or correction to your HMIS record.

If Your Request is Denied: You will be provided written documentation regarding your request and the reason for denial. A copy of all documentation related to your request will also be recorded and saved in your program record. You may appeal this decision and request the CoC review the denial. Regardless of the outcome of the appeal, you have the right to add to your program record a statement of disagreement.

Grievance: You have the right to be heard if you feel that your confidentiality rights have been violated, if you have been denied access to your HMIS records, or if you believe you have been put at personal risk, or harmed. The CoC has established a formal grievance process for you to use in such a circumstance. To file a complaint or grievance, contact us at:

The Butte Countywide Continuum of Care
205 Mira Loma Drive, Suite 50
Oroville, CA 95965
(530) 552-6200
HMISHelp@buttecounty.net

Right to Request Confidential Communications: You have the right to request we communicate with you about appointments or other matters related to your service in a specific way or at a specific location. For example, you can ask that we only contact you at work, or by mail at a post office box. To request confidential communications, you must make your request in writing to your case manager at the agency providing you services or the person in charge of your services. Your request must specify how or where you wish to be contacted.

OTHER RIGHTS

Right to Refuse: In certain circumstances, the ability to provide some services depends on having certain PPI and therefore, we may have to decline or delay providing you with services if you do not disclose the information needed for those services.

To File a Complaint with the Lead Agency: You have the right to file a complaint if you believe staff has not complied with the practices outlined in this Notice. All complaints must be submitted in writing. You will not be penalized in any way for filing a complaint. You may file a complaint with the Butte Countywide Homeless Continuum of Care Coordinator. Contact the Butte Countywide Continuum of Care, 205 Mira Loma Drive, Suite 50, Oroville, CA 95965, in writing, or call (530) 552-6200, or email ButteCoC@buttecounty.net.

ACKNOWLEDGEMENT OF RECEIPT

By signing this form, you acknowledge you have been provided with a copy of the Butte Countywide Homeless Continuum of Care's Privacy Notice. If you have any questions about our Privacy Notice, please contact: Butte Countywide Continuum of Care, 205 Mira Loma Drive, Suite 50, Oroville, CA 95965, in writing, or call (530) 552-6200, or email HMISHelp@buttecounty.net.

I acknowledge receipt of the Butte Countywide Homeless Continuum of Care's Privacy Notice.

Client Name: _____ Client DOB: _____
(Print)

Client Signature: _____ Date Signed: _____
(Sign)

AGENCY PROVIDING COPY OF NOTICE

Agency Name:
Agency Address:
Agency Phone:

Staff Name:_____ Signature: _____
(Print)

INABILITY TO OBTAIN ACKNOWLEDGEMENT: If it is not possible to obtain the client's acknowledgement, describe the good faith efforts made to obtain the client's acknowledgement, and the reasons why the acknowledgement was not obtained:

TO BE COMPLETED ONLY IF NO SIGNATURE IS OBTAINED

_____ _____ _____
Staff Member's Signature Staff Name and Title Printed Date

Appendix B; HMIS Public Notice

Butte Countywide Homeless Continuum of Care

HMIS PUBLIC NOTICE

We collect personal information directly from you for our local Homeless Management Information System (HMIS). We may be required to collect personal information by law or by organizations that give us money to operate this program.

The collection and use of all personal information are guided by strict standards of confidentiality. The only people allowed to see the information we collect are local homeless service providers who are committed to assisting you and keeping your information confidential.

The personal information we collect is important to run our programs, to improve services for persons experiencing homelessness, and to better understand the needs of persons experiencing homelessness. We only collect information we are required to, and consider to be appropriate.

Appendix C; End User Agreement

Contributing HMIS Organization End User Agreement

Butte Countywide Continuum of Care Homeless Management Information System

_____

Agency Name

_____

End User Name (Agency Employee)

The Butte Countywide Homeless Continuum of Care (Butte CoC) Homeless Management Information System (HMIS), is a local information technology system used to collect client-level data, and data on the provision of housing and services to homeless individuals and families. The system enables local homeless service providers to coordinate and streamline client services. HMIS data is required by many state and federal funding sources, and is used to determine funds related to homelessness and homeless services.

As an End User of HMIS, you have a moral and legal obligation to ensure client data is collected, accessed, and used appropriately. Misuse of data can result in you being held legally and criminally liable under both State and federal law. End Users and the Contributing HMIS Organization (CHO) HMIS Administrator must ensure client data is collected, entered, accessed and used only on a need to know and right to know basis.

The Butte CoC is committed to maintaining the confidentiality of client information and protecting clients' rights. To ensure compliance with this obligation, review, and initial each item below. By initialing and signing this form you are indicating you understand and comply with the requirements related to being a HMIS End User:

_____ I understand that I have an obligation to maintain client privacy and to protect and safeguard the confidentiality of a client's Personal Identifiable Information (PII). PII includes, but is not limited to, client's name, address, telephone number, social security number, date of birth, type of care provided, medical condition or diagnosis, veteran status, employment information, and any and all other information relating to the services provided to the client by this or other agencies.

_____ I will receive, complete and pass HMIS training in the HMIS training site before being granted access to the live HMIS program.

_____ I understand once I have access to the live site, I will be required to re-sign this End User Agreement. Additionally, every 6 (six) months, the live site will require me to re-sign this agreement.

_____ I will participate in annual HMIS update training as long as I am an End User.

_____ I have read and will abide by all the HMIS Policies and Procedures, including data standards required by the Data Quality Plan and protocols required by the Security and Privacy Plans.

_____ I understand the HMIS Policies and Procedures, the Data Quality Plan, and the Security and Privacy Plans are dynamic, meaning they can and will be modified, and I am responsible for complying with any changes made to these plans.

_____ I understand that my username and password are for my use only and must not be shared with anyone, including but not limited to another End User, and my agency's CHO HMIS Administrator.

_____ I must take all reasonable means to keep my password secure, including but not limited to never selecting the option to have my browser save my password.

_____ If I am logged into HMIS and need to leave the computer, tablet, phone or other mobile device or work area for any amount of time, I will log off the software, close the browser and lock the device before leaving.

_____ I understand my computer, tablet, phone or other mobile device must have password protected screensavers set at no more than 15 minutes.

_____ If I use a laptop computer, tablet, phone or any other mobile device to enter HMIS data, I will not use that for unauthorized purposes or from unauthorized locations.

_____ I will notify my CHO HMIS Administrator if deadlines appear to be in jeopardy, if the HMIS Software System is not working correctly, or if I have any other questions.

_____ I understand that only authorized End Users and agency CHO HMIS Administrators can view HMIS information, and not all End Users can view all information.

_____ I will ensure HMIS data and client interactions are entering into the system within 3 days.

_____ I will ensure that paper documentation or physical files are complete, secure, and confidential at all times, and when no longer needed, are properly destroyed to maintain confidentiality.

_____ I may only view, obtain, disclose, or use database information necessary to perform my job. As an HMIS user, I understand I may not look up a client in HMIS to know their whereabouts, their history or current information for the purposes of outside inquiries or personal use.

_____ I understand that I can be held legally liable for any unauthorized access, usage, or disclosure of data collected for the purpose of entering into the HMIS database and data held within HMIS as specified in the California Penal Code Section 502 and/or under other State and federal laws.

_____ I agree I will maintain HMIS data in such a way as to protect against revealing the identity of clients to unauthorized agencies, individuals or entities, including but not limited to law enforcement agencies.

_____ I will not discuss client's personal or other information in a public area.

_____ I will not electronically transmit unencrypted client data across a public network. I understand that PII cannot be distributed through email.

_____ Discriminatory comments base on race, color, religion, national origin, ancestry, handicap, age, gender, orientation, are not permitted in HMIS. Profanity and offensive language are not permitted in HMIS.

_____ I will not log into HMIS during non-work hours, or on computers or any device that is not approved by my agency.

_____ If I notice or suspect a security breach within HMIS or related to HMIS data, I must immediately notify my CHO HMIS Administrator. Notification must occur within one (1) hour and in writing.

_____ If I notice or suspect a security breach committed by the CHO HMIS Administrator, I must immediately notify the HMIS Lead Agency. Notification must occur within one (1) hour and in writing.

_____ I will not knowingly enter malicious or erroneous information into HMIS.

_____ The appropriate client Informed Consent form must be completed with each client whose data is to be entered into HMIS and uploaded to the client profile.

_____ I understand that my username and password will terminate should I move employment and will not be passed on to the staff person that replaces me.

_____ I understand these rules apply to all HMIS Users, whatever their work role or position.

_____ I have completed the required criminal background check through my agency. I understand I am not allowed to access HMIS if I have ever had a felony or misdemeanor conviction, been found guilty of or entered a plea of nolo contendere (no contest) to any fraud, identity theft, stalking, human trafficking or related charges.

You are required to maintain strict confidentiality of information obtained through or related to Butte CoC HMIS. Data and information will be used only for legitimate client service and administration of the above-named agency. Any breach of confidentiality or failure to comply with the terms listed above will result, at a minimum, in your immediate and lifelong termination in participation in the Butte CoC HMIS.

_____ _____

End User Signature Date

_____ _____

CHO Administrator Date

Appendix D; Informed Consent

Client Name: _____ Client DOB: _____

Butte Countywide HMIS Client Informed Consent

PERMISSION TO SHARE PROTECTED IDENTIFYING INFORMATION (PII) TO SECURE NECESSARY SERVICES

Please read the following notice and authorization (or ask to have it read to you) before signing.

_____ (Enter your Agency's name in the space) is a Partner Agency in the Butte Countywide Homeless Management Information System (HMIS). HMIS is a shared housing and homeless services database. HMIS operates over the Internet, and uses many security protections to keep your information private and secure.

HOW YOU WILL BENEFIT FROM PROVIDING YOUR CONSENT TO SHARE YOUR PERSONAL INFORMATION:

The information collected in the HMIS is for the purpose of finding out what kind of services you and your family are in need of. The personal information contained in the HMIS database may be shared with Partner Agencies to find and set up the most effective services and resources within the community for you and your family. As you receive services, information will be collected about you, the services provided to you, and the outcomes these services help you to achieve. The information shared may consist of the following Protected Identifying Information (PII):

- Name
- Date of Birth
- Social Security Number
- Gender
- Ethnicity & Race
- Residence Prior to project entry
- Current & historical housed and unhoused status
- Family composition
- Alcohol & Drug history*
- Information about services provided by HMIS particip agencies (including: date, duration, type of service an other similar service information)
- Legal history
- Domestic Violence**
- Income & Non-Cash benefit information
- VI-SPDAT
- Photo
- Veteran Status
- Employment Status
- Disabling condition (physical and/or mental health)

*Alcohol and Drug history information will not prevent you receiving homeless services and/or housing assistance.
**Domestic Violence information is provided by you during your assessment to be on the list for available housing.

Your information will not be shared with any agencies outside of the Butte Countywide HMIS, unless we are required to do so by law.

Right to Decline or Revoke: I understand that I have the right to not share my information or to stop sharing my information at any time by writing to: Housing and Homeless Branch, 202 Mira Loma Drive, Oroville, CA 95965 or e- mailing ButteCoC@buttecounty.net. May also call 530-552-6200 and select option to speak with Housing Navigator or you can inform the agency you are working with and they will email the Housing and Homeless Branch of Butte County Department of Employment and Social Services.

Expiration/Renewal: I understand this Consent is good for 3 years from the date of my signature below OR until I cancel my consent. I understand that if I cancel my Consent, all information about me already in the database will remain, but will become invisible to all of the participating agencies.

Other Rights: I understand that sharing my information is voluntary and I can refuse to sign this consent form. I understand if I refuse to sign this Consent, I will still receive services, but they may be limited or delayed. I understand I have the right to see the client confidentiality policies used by the HMIS Partner Agencies.

Right to a Copy of My Information: I understand that I may have a copy of the information collected in HMIS by Partner Agencies.

Right to a Copy of this Consent: I have right to receive a copy this Consent form.

Authorized Participating Agencies: The current list of Butte Countywide HMIS Participating Agencies is available on the Butte Countywide CoC Website www.buttehomelesscoc.com

List all Dependent children under 18 in household, if any (first and last names):

1. _____ 2. _____

3. _____ 4. _____

5. _____ 6. _____

Please initial ONE of the following levels of consent:

_____I give consent for my/our basic and relevant information to be entered into HMIS and shared with Partner Agencies in the Butte Countywide HMIS. I understand that I may have a copy of the information shared between Partner Agencies.
OR

_____I give consent for my/our basic and relevant information to be entered into HMIS, but **not** shared with Partner Agencies in the Butte Countywide HMIS. The information gathered and prepared by this Agency can be included in the HMIS database.

_____ _____
Client's Signature Date

☐ Verbal Consent obtained by phone (Agency Staff Initials): _____Date: _____

_____ _____ _____
Agency Personnel Name (print) Agency Personnel Signature Date

Note: A separate HIPAA-compliant authorization is required for disclosure of any patient health information, including mental health and drug and alcohol information protected by any State or Federal privacy law including, but not limited to, Health Insurance Portability and Accountability Act ("HIPAA"), 45

C.F.R. parts 160 and 164, California Confidentiality of Medical Information Act ("CMIA"), Civil Codes sections 56-56.16, Welfare and Institutions Code section 5328, or 42 C.F.R. part 2.1 et se

Appendix E; Privacy Notice Quick guide for Organizations in the Butte Countywide Homeless Continuum of Care

Butte Countywide Homeless Continuum of Care

Privacy Notice

Quick Guide for organizations in the Butte Countywide Homeless Continuum of Care

When you meet with a member of our organization or get services from us, you consent to allow us to collect, use, and share information about you for certain reasons. We have a responsibility to protect your information and privacy.

This Privacy Notice summarizes our Privacy Policy. The Privacy Notice and Policy can be found online at https://www.buttehomelesscoc.com/ or you can ask a staff member for a copy.

What information do we collect?

We collect information that can be used to identify you, such as:

- Your name, address, date of birth.
- Contact information.
- Identification numbers.
- Photos or videos.
- Information about services you received.

Why do we collect and share your information?

We collect, use, or share your information to:

- Provide or coordinate services.
- Collect payments.
- Run the organization.
- Create data that can't identify you.
- Support research.
- Follow local, state, and federal laws.
- Follow court orders, respond to threats, and ensure public safety.

We will ask for your written or verbal consent to use or share your information for any purpose not listed above, or if the law requires it.

What other steps do we take to protect your privacy?

In addition to following local, state, and federal laws, we will:

- Assist you if you need help or translation, as required by law.
- Explain and share our Privacy Notice and the Privacy Policy. This Notice summarizes the Policy.
- Only collect the information we need.
- Have a plan for keeping information in good order.
- Share the least amount of information needed to complete a task.
- Allow you to review and correct your information and explain if your request is denied.
- Have a plan and train staff to handle questions, complaints, or a data breach. The Privacy Policy can be changed at any time. Changes can apply to information that has already been collected.

For a list of organizations that are part of the Butte Countywide Homeless Continuum of Care, please visit https://www.buttehomelesscoc.com/ or ask a staff member for a copy.

Appendix F; Acknowledgement of Receipt

Butte Countywide Homeless Continuum of Care

Verification of Receipt and Understanding of the

Butte Countywide Homeless Continuum of Care HMIS Privacy Security Plan

The Butte Countywide Homeless Continuum of Care (CoC) Homeless Management Information System (HMIS) Privacy and Security Plan contains important information regarding the expectations of Contributing HMIS Organizations (CHOs) and HMIS End Users. All HMIS Users must read, initial and sign this form:

_____I acknowledge that I have received a copy of the Butte Countywide Continuum of Care's HMIS Privacy and Security Plan. I understand it is my responsibility to read and comply with policies contained in this plan as well as any revisions made to it. I also understand if I need additional information, or if there is anything that I do not understand in the Plan, I should contact my agency's CHO Administrator.

_____I understand that this Plan reflects policies, practices, and procedures in effect on the date of publication and that it supersedes any prior plan. I further understand that rules, policies, expectations referred to in the Plan are evaluated and may be modified at any time, with or without notice. I acknowledge that the Plan will be updated by the CoC's HMIS/CES Committee and it is my responsibility to be aware of and to adhere to the changes in the Plan as they occur.

End User Name(Print): _____

End User Agency Name: _____

End User Signature: _____ Date: _____

Appendix G; HMIS Quarterly Compliance Checklist

Butte County CoC HMIS Quarterly Compliance Checklist	☐ Quarter 1, due 4/30	CHO Agency Name:	
	☐ Quarter 2, due 7/31	CHO Administrator Name:	
	☐ Quarter 3, due 10/31	Date Completed:	
	☐ Quarter 4, due 1/31	Date Sent:	

Workstation Security Standards

In partnership with the Butte Countywide Continuum of Care (CoC), Clarity Human Services Software, a division of Bitfocus, Inc., administers the County's Homeless Management Information System (HMIS), a shared database software application which collects, client-level information related to homelessness in the County. Client information is collected in HMIS by Contributory HMIS Organizations (CHO or collectively, CHOs). Information collected is used by the HUD and the CoC to identify national and local patterns and trends in homelessness over time; to conduct needs assessments and prioritize services for certain homeless and low-income subpopulations; to enhance inter-agency coordination; and to monitor and report on the quality of housing and services. This Compliance Certification Checklist is to be completed and certified quarterly by every CHO Administrator according to the schedule outlined below. Each Agency workstation used for HMIS data collection, data entry, or reporting must be certified compliant. Any identified compliance issues must be resolved within thirty (30) calendar days. Upon completion, the original signed copy of this checklist should be retained in the records of the HMIS CHO named above for a minimum of seven (7) years. Additionally, a copy should be emailed to the HMIS Lead at HMIShelp@buttecounty.net with the subject line: "Quarterly compliance check for _____(name of CHO).

Compliance Certification Schedule:

- Quarter 1 (due by April 30th): ALL Active HMIS Users and Workstations Q1 (Jan-Mar)
- Quarter 2 (due by July 31st): ALL Active HMIS Users and Workstations Q2 (Apr-June)
- Quarter 3 (due by October 31st): ALL Active HMIS Users and Workstations Q3 (July-Sep)
- Quarter 4 (due by January 31st): ALL Active HMIS Users and Workstations Q4 (Oct-Dec)

Workstation Security Standards

1. The Butte CoC HMIS Privacy Notice is visibly posted at each HMIS intake desk (or comparable location). If the workstation is not in a fixed location HMIS Privacy Statement is being provided as a handout.
2. Each HMIS workstation computer is in a secure location where only Authorized Persons* have access.
3. Each HMIS workstation computer is password-protected and locked when not in use. (Changing passwords on a regular basis is recommended)
4. Documents printed from HMIS are sent to a printer in a secure location where only Authorized Persons have access.
5. Non-authorized persons are unable to view any HMIS workstation computer monitor.
6. Each HMIS workstation computer has anti-virus software with current virus definitions (i.e., within the past twenty-four (24) hours), and each HMIS workstation computer has had a full system scan within the past week.
7. Each HMIS workstation computer has and uses a hardware or software firewall.

8. Unencrypted protected personal information ("PPI") ** has not been electronically stored or transmitted in any fashion (including, without limitation, by hard drive, flash drive, emails, etc.) (Encrypted hard drives are recommended)
9. Hard copies of PPI (including, without limitation, client files, intake forms, printed reports, etc.) are stored in a physically secure location.
10. Each HMIS workstation computer password information, including each Authorized Person's user identification information, is kept electronically and physically secure.
    - No passwords for HMIS have been saved on the computer, browser or server.
    - No log-in information (e.g. passwords, user names) is written down or have been shared.

**An "Authorized Person" means a CHO authorized agent or representative (a HMIS End User or simply an End User) who has completed HMIS training.*
*** Protected Personal Information (PPI) is defined as client-level identifying information, including, without limitation, information about names, birth dates, gender, race, social security number, phone number, residence address, photographic likeness, employment status, income verification, public assistance payments or allowances, food stamp allotments, or other similar information*

CHO Administrator Works station Checklist

Instructions: For each HMIS workstation at your agency fill in the workstation location or end username. Verify checklist items 1 through 10b on the for the workstation and check (✓) the box to confirm the verification is complete. Fill in additional notes/comments and compliance issues as needed. Attach additional pages if necessary. Return this form to HMIShelp@buttecounty.net

No	***Workstation Location Or End User Name***	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**10a**	**10b**	***Notes***
1														
2														
3														
4														
5														
6														

No	*Workstation Location Or End User Name*	1	2	3	4	5	6	7	8	9	10	10a	10b	*Notes*
7														
8														
9														
10														
11														
12														

Workstation Security Compliance Issues Identified	*Corrective Action Taken to Resolve Security Compliance Issue*

Workstation Security Compliance Issues Identified	*Corrective Action Taken to Resolve Security Compliance Issue*

CHO Administrator Works station Checklist

I have verified that, (initial):

_____ Each End User workstation / device used to access HMIS has completed the Workstation Security Standards review.

_____ All devices used to access HMIS by CHO End Users were provided and authorized for use by CHO.

_____ Each End User is completing the Butte CoC HMIS Informed Consent with clients.

_____ Each End User requires access to HMIS to perform their assigned duties.

_____ No unauthorized access to HMIS or confidential legally protected client data was divulged to unauthorized third parties.

_____ Incident of unauthorized access has been reported to HMIS Lead Agency and impacted clients have been notified.

Date of Incident: _____ Name of HMIS Lead Agency Staff Member Informed: _____

_____	_____	_____
CHO Administrator Name (Print)	CHO Administrator Signature	Date
_____	_____	_____
CHO Agency Director Name (Print)	CHO Agency Director Signature	Date

Appendix H; HMIS Lead Privacy & Security Compliance Checklist

Butte Countywide Homeless Continuum of Care

HMIS Lead Privacy & Security Compliance Checklist

Agency Official Name	Security Officer Name

_____ (Int.) Agency has the HUD Public Notice posted in an area visible to clients.

_____ (Int.) Agency has an HMIS Privacy Notice that complies with the requirements set forth by the CoC HMIS Operating Policies and Procedures and is available to all clients.

_____ (Int.) Agency has a copy of the HUD Public Notice and the Privacy Notice on its website.

_____ (Int.) Client files with hard copy data that includes client identifying information are protected behind one lock, at a minimum, from unauthorized access.

_____ (Int.) Offices that contain client files are locked when not occupied.

_____ (Int.) Client files are not left visible to unauthorized individuals.

_____ (Int.) Agency has adopted the Informed Consent and requests this for every client.

_____ (Int.) HMIS workspaces are configured to support the privacy of client interaction and data entry.

_____ (Int.) User accounts and passwords are not shared or left visible for others to see.

_____ (Int.) End Users do not save HMIS reports with identifying client information on computers, laptops, tablets or other media devices.

_____ (Int.) All HMIS workstations, including laptops and remote workstations, have virus protection and automatic updates.

_____ (Int.) End Users are not accessing the HMIS on a public computer, personal device or from an internet connection that is not secured.

_____ (Int.) Agency has a documented plan for remote access if End Users are accessing the HMIS outside of the office setting.

Findings : _____

_____

_____

Corrective Actions: _____

_____

_____

Deadline for Completion: _____

_____	_____
Security Official Printed Name	Agency Official Printed Name
_____	_____
Security Official Signature	Agency Official Signature
_____	_____
Date (mm/dd/yy)	Date (mm/dd/yy)

Appendix I; Background Check Template

Current Date

In accordance within the terms and conditions of the Contributing HMIS Organization Participation Agreement

(CHO) between Your Agency Name and Butte County, Department of Employment and Social Services (HMIS Lead Agency), the HMIS Policies & Procedures and the End User Agreement, I hereby certify and attest that a criminal background check for HMIS End User, Name of User, employee of Your Agency Name, was completed on Insert Date, and Name of User, has no criminal history that precludes them from accessing the Butte Countywide Continuum of Care's HMIS.

I additionally certify, Your Agency Name will retain the results of the background check in the employee's personnel file.

Verified By:

_____

Name, Title Signature Date

Appendix J; Authorized Representative

Butte Countywide Homeless Continuum of Care

HMIS Authorized Representative (AR) Form

An Authorized Representative (AR) is someone you choose to act on your behalf and manage your information in the Butte Countywide Homeless Continuum of Care's (CoC) Homeless Management Information System (HMIS). Choosing an AR is optional, and you decide how much control the AR has over your information in HMIS. An AR can speak with HMIS participating agencies on your behalf.

You can choose to allow either; HMIS participating agencies to only provide information to your AR, or to allow your AR to update your HMIS information on your behalf. It is important when choosing an AR, to choose someone you trust. You **can** choose a family member, friend, or other trusted person. You **cannot** choose an agency or agency staff member.

ARs must be at least 18 years old and must provide proof of their identity any time they speak with a HMIS participating agency. The person you choose as your AR will be listed in your HMIS profile, until you choose to revoke authorization. You may remove an AR at any time, verbally or in writing. You must provide all information required below, failure to provide all required information will result in the person not being listed as your AR.

This form must be completed in the presence of an employee of an HMIS Participating Agency and all parties must be physically present.

Client Information	
Client Full Name	Client HMIS Unique Identifier
Client Date of Birth	
Authorized Representative (AR) Information	
AR Full Name (Last, First)	AR Password (New form must be completed to change a password)
AR Date of Birth	AR Phone Number
AR Mailing Address	
Level of HMIS Authorization Granted to AR	
☐ HMIS Participating Agencies can only provide information to AR. AR is ***NOT*** able to change or update my information in HMIS or CES. ☐ HMIS Participating Agencies can provide information to AR, and AR ***IS*** able to change or update my information in HMIS or CES.	
NOTE: HIPAA restrictions prevent us from discussing the client's individual health information with the authorized representative unless the representative has power of attorney for the client	

Butte Countywide Homeless Continuum of Care

HMIS Authorized Representative (AR) Form

HMIS User Completing Form and Entering into HMIS	
HMIS User: By signing below, I swear under penalty of perjury that the client willingly requested and signed this form. I have explained the concept of an AR and the levels of authorization the client can choose. The client has indicated understanding. The client understands they can withdraw consent, without informing the AR, at any time. I will upload this form and update HMIS within 24 hours of completion. I have provided a completed copy of this form to the client and the AR.	
HMIS User Full Name (print)	HMIS User Agency/Organization
HMIS User Signature	Date

Client Authorization	
Client: By signing below, I acknowledge I have willingly signed this form, and no one has pressured me to do so. I understand the concept of an AR and the level of authorization I have granted my designated AR. I understand I can withdraw consent at any time, without the AR's knowledge or approval. I have been given a copy of this completed form.	
Client Signature	Date
Client Phone Number	☐ I am revoking AR authorization effective immediately. Date: _____

AR Authorization	
Authorized Representative: By signing below, I acknowledge I understand the concept of an Authorized Representative and the level of authorization I have been granted by the client. I understand the client listed in this form can withdraw their consent at any time, without my knowledge or approval. I have been given a copy of this completed form.	
AR Signature	Date
AR Phone Number	

Revocation of AR Authorization (To be completed by HMIS User ONLY)		
☐ Revoked in Person ☐ Revoked Verbally	☐ Client profile updated ☐ Uploaded form to HMIS	HMIS User Name: _____ HMIS User Agency: _____