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 November 18, 2024

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, a key purpose of HMIS is to relieve clients in crisis from the responsibility of managing their own data, allowing service providers to take on that role instead. Thus, allowing clients to focus on 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, 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 changed 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 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 are responsible for preventing the 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

The 2004 HMIS Data and Technical Standards Final Notice , quoted below, permit 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.
- 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 accessing services through the Butte Countywide Homeless Continuum of Care, and to better understand the needs of persons experiencing homelessness. We only collect information we are required to, and consider to be appropriate.

A copy of our Privacy Notice describing our privacy practice is available to all clients upon request.

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
10/07/2024	1.0	HMIS/CES Committee	Approved by HMIS/CES Committee
11/18/2024	1.0	CoC	Approved by the CoC

Appendix A; HMIS Privacy Notice

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

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														

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

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 J; Authorized Representative