HMIS PRIVACY
&
SECURITY PLAN

Sacramento County

Continuum of Care (CoC)

PRIVACY & SECURITY

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

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

HMIS Privacy and Security Plan

Adopted by the Sacramento County Continuum of Care (December 2023)

Contents

Introduction

The Homeless Management Information Systems (HMIS) Lead Agency is responsible for overseeing HMIS privacy and security. The HMIS Lead Agency may and have delegated some specific duties related to maintaining HMIS privacy and security to the HMIS System Administrator. The HMIS System Administrator is responsible for preventing degradation of the HMIS resulting from viruses, intrusion, or other factors within the 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. The HMIS Partner Agencies are responsible for preventing degradation of the HMIS resulting from viruses, intrusion, or other factors within the agency's control and for preventing inadvertent release of confidential specific client-specific information through physical, electronic, or visual access to End User workstations. Each Partner Agency is responsible for ensuring it meets the Privacy and Security requirements detailed in the HUD HMIS Data and Technical Standards. Partner Agencies will conduct a thorough review of internal policies and procedures regarding HMIS annually.

Privacy

Privacy Plan Overview

On July 30, 2004, the US Department of Housing and Urban Development (HUD) released the standards for Homeless Management Information Systems (***Federal Register / Vol. 69, No. 146 / Notices***) and on December 9, 2011, HUD released HMIS Requirements Proposed Rule (***Federal Register / Vol. 76, No. 237 / Friday, December 9, 2011 / Proposed Rules***).

These standards outlined the responsibilities of the HMIS System Administrator and the HMIS Partners Agencies which participate in an HMIS. This section describes the Privacy Plan of the Sacramento HMIS System. We intend our policy and plan to be consistent with the HUD standards. All end users, partner agencies, and system administrators must adhere to this Privacy Plan.

We intend our Privacy Plan to support our mission of providing an effective and usable case management tool. We recognize that clients served by individual agencies are not exclusively that "agency's client" but instead is truly a client of the Sacramento Continuum of Care (CoC). Thus, we have adopted a Privacy Plan which supports an open system of client-level data sharing amongst agencies.

The core tenant of our Privacy Plan is the Baseline Privacy Statement. The Baseline Privacy Statement describes how client information may be used and disclosed and how clients can get access to their information. Each agency must either adopt the Baseline Privacy Statement or develop a Privacy Statement that meets and exceeds all minimum requirements set forth in the Baseline Privacy Statement (this is described in the Agency Responsibilities section of this Privacy Plan). This ensures that all partner agencies who participate in the HMIS are governed by the same minimum standards of client privacy protection.

Baseline Privacy Statement: This is the main document of this Privacy Plan. This document outlines the minimum standard by which an agency	*REQUIRED* Agencies must adopt a privacy statement which meets all minimum standards. It is strongly recommended to post this Statement on

collects, utilizes, and discloses information.	your Agency's local website (if available).
Consumer 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 a Consumer Notice.
Consumers Informed Consent & Release of Information Authorization: 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.	*REQUIRED* Client Signatures are required prior to inputting their information in HMIS.

HMIS User Responsibilities

A client's privacy is upheld only to the extent that the end users and direct service providers protect and maintain their privacy. The role and responsibilities of the end user cannot be over-emphasized. A user is defined as a person that has direct interaction with a client, their data, and HMIS access. (This could potentially be any person at the agency: staff member, contractor, consultant, etc.)

Users have the responsibility to:

- Understand their agency's Privacy Statement;
- Be able to explain their agency's Privacy Statement to clients;
- Follow their agency's Privacy Statement;
- Know where to refer the client if they cannot answer the client's questions;
- Must complete Consumers Informed Consent & Release of Information Authorization with client prior collecting HMIS data;
- Present their agency's Privacy Statement client before collecting any information;
- Uphold the client's privacy in the HMIS.

Partner Agency Responsibilities

The 2004 HUD HMIS Standards emphasize that it is the partner agency's responsibility for upholding client privacy. All partnered agencies must take this task seriously and take time to understand the legal, ethical, and regulatory responsibilities. This Privacy Plan and the Baseline Privacy Statement provide guidance on the minimum standards by which agencies must operate if they wish to participate in the HMIS.

Meeting the minimum standards in this Privacy Plan and the Baseline Privacy Statement are required for participation in the HMIS. Any partner agency may exceed the minimum standards described and are encouraged to do so. Partnered agencies must have an adopted Privacy Statement which meets the minimum standards before data entry into the HMIS can occur.

Partners agencies 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 Baseline Privacy Statement (examples: Substance Abuse Providers covered by 24 CFR Part 2, HIPPA Covered Agencies, Legal Service Providers).
- Review the 2004 HUD HMIS Privacy Standards (***Federal Register 45888/Vol. 69, No. 146/July***

30, 2004/Notices)

- Adopt and uphold a Privacy Statement which meets or exceeds all minimum standards in the Baseline Privacy Statement as well as all industry privacy standards. The adoption process is to be directed by the individual agency. Modifications to the Baseline Privacy Statement must be approved by the HMIS Committee.
- Ensure that all clients are aware of the adopted Privacy Statement and have access to it. If the agency has a website, it is strongly recommended that the agency publish the Privacy Statement 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 Statement can meet the User Responsibilities.

Each HMIS Partner Agency must have a Privacy Statement that describes how and when the Partner Agency may use and disclose clients' Protected Personal Information (PPI). PPI is any information about living homeless client or homeless individual that: (1) Identifies, either directly or indirectly, a specific individual; (2) can be manipulated by a reasonably foreseeable method to identify a specific individual; or (3) can be linked with other available information to identify a specific individual.

Partner Agencies may be required to collect some PPI by law, or by organizations that give the agency money to operate their projects. PPI is also collected by Partner Agencies to monitor project operations, to better understand the needs of people experiencing homelessness, and to improve services for people experiencing homelessness. Partner Agencies are permitted to collect PPI only with a client's written or electronic consent.

Partner Agencies may use and disclose client PPI to:

- Verify eligibility for services;
- Provide clients with and/or refer clients to services that meet their needs;
- Manage and evaluate the performance of programs;
- Report about program operations and outcomes to funders and/or apply for additional funding to support agency programs;
- Collaborate with other local agencies to improve service coordination, reduce gaps in services, and develop community-wide strategic plans to address basic human needs;
- Participate in research projects to better understand the needs of people served.

Partner Agencies may also be required to disclose PPI for the following reasons:

- When the law requires it;
- When necessary to prevent or respond to a serious and imminent threat to health or safety;
- When a judge or administrative agency orders it.

Partner Agencies are obligated to limit disclosures of PPI to the minimum necessary to accomplish the purpose of the disclosure. Uses and disclosures of PPI not described above may only be made with a client's written consent. Clients have the right to revoke consent at any time by submitting a request in writing.

HMIS end users may respond to an oral request from a law enforcement officer for PPI for the purpose of identifying or locating a suspect, fugitive, material witness or missing person. Nonetheless, the only PPI that may be shared is the name, address, date of birth, place of birth,

social security number, and distinguishing physical characteristics of the individual. No programmatic information including program enrollments, services provided, recent field contacts, or the like may be shared.

Clients also have the right to request in writing:

- A copy of all PPI collected;
- An amendment to any PPI 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 should be noted in the project records);
- An account of all disclosures of client PPI;
- Restrictions on the type of information disclosed to outside partners;
- A current copy of the Partner Agency's privacy statement.

Partner Agencies may reserve the right to refuse a client's request for inspection or copying of PPI 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 Partner Agency believes that disclosure of the information would be reasonably likely to endanger the life or physical safety of any individual.

If a client's request is denied, the client should receive a written explanation of the reason of the denial. The client has the right to appeal the denial by following the established Partner Agency grievance procedure or the Sacramento CoC grievance procedure[1]. 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 Partner Agency shall disclose the statement of disagreement whenever it discloses the disputed PPI.

All individuals with access to PPI are required to complete an HMIS certification quiz on HMIS procedures as a new user and/or annually and pass with a score of 70% or above. Individuals who fail to score 70% or above on the quiz will be required to re-take the quiz or attend an HMIS training.

Partner Agency Privacy Statements 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 Statement 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 Statement must be made available to clients upon request.

This document should, at a minimum, reflect the baseline requirements listed in the HMIS Data and Technical Standards Final Notice, published by HUD in July 2004 (***Federal Register 45888/Vol. 69, No. 146/July 30, 2004/Notices***) and the latest revised in FY 2022 HMIS Data Standards (**https://www.hudexchange.info/programs/hmis/hmis-data-standards**).

In any instance where this Privacy Statement is not consistent with the HUD standards, the HUD standards take precedence. Should any inconsistencies be identified, please immediately notify the

[1] The Sacramento CoC grievance procedure is available upon request.

Sacramento HMIS Lead Agency, using the contact information below.

All questions and requests related to this Privacy Statement should be directed to the HMIS Department at Sacramento Steps Forward. Email HMIS@sacstepsforward.org.

HMIS Lead Agency: System Administrator Responsibilities

HMIS Lead Agency has the responsibility to:

- Adopt and uphold a Privacy Plan which meets or exceeds all minimum standards in the Baseline Privacy Statement;
- Train and monitor all end users upholding system privacy;
- Audit partner agencies to ensure adherence to their adopted Privacy Plan;
- Develop action and compliance plans for partner agencies that do not have adequate Privacy Statements;
- Maintain the lead CoC HMIS Website to keep all references within the Baseline Privacy Statement up to date;
- Provide training to partner agencies and end users on this Privacy Plan;
- Dispose of or, in the alternative, to remove identifiers from PPI that is not in current use seven years after the PPI was created or last changed;
- Ensure partner agencies obtain Consent & Release of Information Authorization from the client when their consent is no longer valid. The release of consent is valid for seven (7) years from the date of the client signature.

System Security

Security Plan Overview

HMIS security standards are established to ensure the confidentiality, integrity, and availability of all HMIS information. The security standards are designed to protect against any reasonably anticipated threats or hazards to security and must be enforced by the System Administrator, agency 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 (***Federal Register 45888/Vol. 69, No. 146/July 30, 2004/Notices***) as well as local legislation pertaining to maintaining an individual's personal information. At this time, in December 2011, HUD has released proposed regulations pertaining to HMIS Security (***Federal Register 76917/Vol. 76, No. 237/December 9, 2011/ Proposed Rules***). These regulations are not yet in force and sufficient guidance has not been given to enact the policies.

Meeting the minimum standards in this Security Plan is required for participation in the HMIS. Any partner agency may exceed the minimum standards described in this plan and are encouraged to do so. All Partner Agency 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 partner agencies must apply the security standards addressed in this Security Plan to all the systems where PPI 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, mobile devices, mainframes, and servers.

All partner agencies, including the HMIS Lead Agency will be monitored by the HMIS System

Administrator annually to ensure compliance with the Security Plan. Partner agencies that do not adhere to the security plan will be given a reasonable amount of time to address any concerns. Egregious violations of the security plan may result in immediate termination of a partner agency or end user access to the HMIS as determined by the HMIS Lead Agency and the HMIS System Administrator.

Security Personnel

The HMIS Lead Agency may designate a Lead Security personnel or Lead Team to oversee HMIS privacy and security. The HMIS Lead Agency has designated the SSF's HMIS Department HMIS System Administrators as the single point-of-contact person or entity who is responsible for annually certifying that Partner Agencies adhere to the Security Plan, as well as testing the CoC's security practices for compliance.

Lead Security Personnel or Lead Team

- May be an HMIS System Administrator or another employee, volunteer or contractor designated by the HMIS Lead Agency who has completed the HMIS trainings that covers Privacy and Security issues and is adequately skilled to assess HMIS security compliance;
- Assesses security measures in place prior to establishing access to HMIS for a new Partner Agency;
- Reviews and maintains file of each Partner Agency annual compliance certification checklists;
- Conducts security audit of all Partner Agencies, on an as needed basis.

Partner Agency

- Conducts and report to the HMIS System Administrator a security audit for any workstation or work device that will be used for HMIS purposes;
  - No less than annually for all partner agencies HMIS workstations or work device, AND
  - Prior to issuing an employee email, AND
  - Any time an existing user changes to a new workstation or device.
- Continually ensures each workstation or work device within the Partner Agency used for HMIS data collection or entry is adequately protected by a firewall and antivirus software (per Technical Safeguards – Workstation Security);
- Completes the annual Compliance Certification Checklist and provide the Checklist to the HMIS System Administrator.

Upon request, the HMIS Lead Agency may be available to provide security guidance to Partner Agencies who do not have the staff capacity or resources to fulfill these duties.

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 HMIS trainings and/or passed the HMIS certification quiz 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 Partner Agency staff members or volunteers. A password protected automatic screen saver will be enabled on any computer used for HMIS data entry.
- Printer location – Documents printed from HMIS must be sent to a printer in a secure location

where only authorized persons have access.

- PC 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 Partner Agency 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 a set period of device inactivity.

Technical Safeguards

Workstation & Mobile Device 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 or mobile devices.
- Partner Agency Security personnel will confirm that any workstation or mobile device accessing HMIS have antivirus software with current virus definitions. Virus protection must include automated scanning on the system where the HMIS application is accessed.
- Partner Agency Security personnel will confirm that any workstation or mobile device accessing HMIS has and uses a hardware or software firewall; either on the workstation or mobile device itself if it accesses the internet through a modem or on the central server if the workstations or mobile devices access the internet through the server.
- Partner Agency Security personnel will confirm that any workstation or mobile device accessing HMIS is configured with the session idle limit to 15 minutes. This setting controls how much time a workstation can be idle before it automatically logs out or is set to sleep.

Establishing HMIS User IDs and Access Levels

- The HMIS System Administrator, in conjunction with the Partner Agency Security personnel will ensure that any prospective end user reads, understands, and signs the HMIS End User Agreement annually. The HMIS System Administrator will maintain a file of all signed HMIS End User Agreements.
- The Partner Agency HMIS Security personnel is responsible for ensuring that all agency end user have completed mandatory training that covers HMIS Privacy, Security and Ethics, End User Responsibilities, and Workflow issues, prior to being provided with a User ID to access HMIS.
- End users must review and sign an HMIS End User Agreement within the HMIS System on an annual basis.
- All end users will be issued a unique User ID and password. Sharing of User IDs and passwords by or among more than one end user 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 create the new User ID and notify the User ID owner of the temporary password via their work email address.
- All end users are required to have a valid and working email address. Email addresses that are not associated with the partner agency email domain will not be accepted.
- When the Partner Agency determines that it is necessary to change an end user's access level, the HMIS System Administrator will update the end user's access level as needed.

User Authentication

- User IDs are individualized and the 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 meet the minimum requirements of:

- At least 8 characters including one uppercase character (A through Z), one lowercase; character (a through z), one number (0 through 9), one special character (!@#$()%^&*);
- Passwords cannot have: any spaces, the word “clarity”, “abc” or “123”, more than two consecutive characters, or your first name, last name, or username;
- The system will not allow you to recycle any of your prior three passwords.

- End Users will be prompted by the software to change their password every 30 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 (3) consecutive unsuccessful attempts to log in will disable the User ID until the password is reset. End users can reset passwords by using the ‘Forgot Password’ option on the HMIS login site or by contacting the HMIS System Administrator.
- End users must log out from HMIS and either lock or log off their respective workstations or devices when unattended.
- A password protected screensaver or automatic lock must be set after a period of 15 minutes of inactivity.

Rescinding User Access (per Appendix A: Data Breach Policy and Procedures)

- The Partner Agency 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 30 days or more.
- Any end user who is found to have misappropriated client data (identity theft, releasing personal client data to any unauthorized party), shall have HMIS privileges revoked.
- The HMIS System Administrator is empowered to permanently revoke a Partner Agency’s access to HMIS for substantiated noncompliance with the provisions of these Security Standards, the Sacramento HMIS Policies and Procedures, or the HMIS Privacy Statement that resulted in a release of PPI.

Establishing Action Plan to Preventing Data Breaches

The policy and procedures described in Appendix A: Data Breach Policy and Procedures are intended to address any privacy and security incidents. Following the reporting and investigation of a privacy and security incident occur the following procedures are to be followed for prevention, to the greatest degree possible:

1. Within one (1) business day after the HMIS System Administrator receives notice of the security or privacy concern, the HMIS System Administrator and Partner Agency Security personnel 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 will describe how the security or privacy concern was determined and identify safeguards that were/are missing or ineffective. The action plan shall be implemented as soon as possible, and the total term of the plan must not exceed thirty (30) days.

2. If the Partner Agency is not able to meet the terms of the action plan within the time allotted, the HMIS System Administrator, in consultation with the Sacramento Continuum of Care Advisory Board, may elect to terminate the Partner Agency's access to HMIS. The Partner Agency may appeal to the CoC Advisory Board for reinstatement to HMIS following completion of the requirements of the action plan.
3. In the event by the Partner Agency Security Personnel, if substantiated release of PPI in noncompliance with the provisions of these Security Standards, the Sacramento HMIS Policies and Procedures, or the Partner Agency Privacy Statement, the Partner Agency Security Personnel will:
    a. Immediately make a reasonable attempt to notify all impacted individual(s).
    b. The HMIS Administrator must approve of the method of notification and the Partner Agency Security Personnel must provide the HMIS System Administrator with evidence of the partner agency's notification attempt(s).
    c. If the HMIS System Administrator is not satisfied with the Partner Agency's efforts to notify impacted individuals, the HMIS System Administrator will attempt to notify impacted individuals at the Partner Agency's expense.
4. In the event by the HMIS Lead Agency, if substantiated release of PPI in noncompliance with the provisions of these Security Standards, the Sacramento HMIS Policies and Procedures, or the Partner Agency Privacy Statement, the HMIS Administrator will:
    a. Immediately make a reasonable attempt to notify all impacted individual(s).
    b. Immediately work with their Information Technology (IT) vendor to determined and identify safeguards that were/are missing or ineffective.
5. The HMIS Lead Agency and the HMIS System Administrator will notify the appropriate body of the CoC of any substantiated release of PPI in noncompliance with the provisions of these Security Standards, the HMIS Policies and Procedures, or the Partner Agency Privacy Statement.
6. The HMIS Lead Agency and HMIS System Administrator will maintain a record of all substantiated releases of PPI in noncompliance with the provisions of these Security Standards, the Sacramento HMIS Policies and Procedures, or the Partner Agency Privacy Statement for seven (7) years.
7. The Sacramento CoC reserves the right to permanently revoke a Partner Agency's access to HMIS for substantiated noncompliance with the provisions of these Security Standards, the Sacramento HMIS Policies and Procedures, or the Partner Agency Privacy Statement that resulted in a release of PPI.

Disposing of Electronic, Hardcopies, Etc.

- Computer: All technology equipment (including computers, mobile devices, printers, copiers, and fax machines) used to access HMIS and which will no longer be used to access HMIS will have the 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.
- Hardcopies: For paper records, shredding, burning, pulping, or pulverizing the records so that PPI is rendered essentially unreadable, indecipherable, and otherwise cannot be reconstructed.
- Mobile Devices: 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.

Other Technical Safeguards

- HMIS System Administrator shall develop and implement procedures for managing new, retired, and compromised HMIS account credentials.
- The Partner Agency Security personnel shall develop and implement procedures for managing new, retired, and compromised local system account credentials.
- The Partner Agency Security personnel shall develop and implement procedures that will prevent unauthorized users from connecting to private agency networks.
- Unencrypted PPI may not be stored or transmitted in any fashion—including sending file attachments by email or downloading reports including PPI to a flash drive, to the end user's desktop or to an agency shared drive. All downloaded files containing PPI 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 Sacramento CoC 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 CoC'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 Administrator 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. This plan should include the following provisions for local usage:
  - Account information – Account numbers and contact information for internet service providers, support contracts, and equipment warranties.
  - Minimum computer equipment and connectivity needs – A list of the computer equipment or internet service provider (ISP) contact information 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 local network access.

Workforce Security

HMIS Access for Persons with Lived Experience

Sacramento CoC has a shared HMIS system providing HMIS end users with access to client's current or past history from other agencies. Partner agencies have sought to hire individuals with lived experience of homelessness or who are currently experiencing homelessness. The individuals may be provided access to the HMIS. Nonetheless, because of the broad access to clients' current or past history to which these individuals will have access, they should be emphasized of their obligations to comply per Homeless Management Information System (HMIS) End-User Agreement.

Background Check

HMIS User Background Check Requirements

The Sacramento CoC recognizes the sensitivity of the data in the HMIS, and therefore requires that the individuals responsible for accessing the HMIS be subject to a criminal background check. The background check must include local and state records; agencies are strongly encouraged to include federal records as well. A background check may be conducted only once for each person unless otherwise required and the clearance &/or results of the background check must be retained in the employee's personnel file.

No prospective end user will be given a HMIS access if he or she has entered a plea of nolo contendere (no contest) or has been found guilty of any fraud (including identity theft) or stalking related felony crimes punishable by imprisonment of one year or more in any state.

Partner Agency Procedure

Partner 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 (including identity theft) or a stalking-related crime in any state. In the broadest sense, fraud is an intentional deception made for personal gain or to damage another individual.

- All end users should have had a background check completed prior to access being requested to the HMIS by a Partner Agency.
- Criminal background checks must be completed on all new end users, and the "Background Check Review and Verification Statement" per HMIS Staff Verification for HMIS Access form must be verified. Stated form must be submitted to the local Lead Agency System Administrator prior to end users gaining access to the HMIS.
- Background checks that return with a criminal history should be carefully considered prior to give an employee access to client information.

HMIS Lead Agency Procedure

HMIS System Administrator must ensure criminal background verification. The partner agency 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.

A staff member's background check revealing a history of following crimes related to identity theft or fraud should not be given access to the HMIS. The "Background Check Review and Verification Statement" must only be verified of staff's background check doesn't reveal a history of following crimes related to identity theft or fraud:

- **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 a 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 upfront or a credit card number upfront, 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.

Reporting Security Incidents (per Appendix A: Data Breach Policy and Procedures)

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 procedures described per Appendix A: Data Breach Policy and Procedures will be followed.

Privacy and Security Monitoring

New HMIS Partner Agency Site Security Assessment

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

Annual Security Audit

- HMIS System Administrator will schedule the annual security audit in advance with the Partner Agency Security Personnel.
- The Partner Agency Lead Security personnel must complete the annual security audit truthfully and accurately in accordance with the baseline standards.
- The Partner Agency Lead Security personnel will ensure all workstations and work devices used to access HMIS are equipped with the following computer systems:
- Virus Protection and System Updates;
- Firewalls;
- Physical Access, meaning when workstations and work devices are not in use and staff

are not present, steps should be taken to ensure that it is secure and not accessible by unauthorized individuals.

- If areas are identified that require action due to noncompliance with these standards or any element of the Sacramento HMIS Policies and Procedures, the Partner Agency Lead Security personnel will note these on the Security Audit Checklist, and the Partner Agency Security personnel and/or HMIS System Administrator will work to resolve the action item(s) within fifteen (15) business days.
- Any 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 and the findings, action items, and resolution summary has been reviewed and signed by the Agency's Executive Director (or executive-level designee) and forwarded to the HMIS System Administrator.

Appendices

Appendix	Title
Appendix A	Data Breach Policy and Procedures

Appendix A: Data Breach Policy and Procedures

In accordance with the Sacramento CoC Privacy & Security Plan, any HMIS end user found to be in violation of privacy and security protocols ("data breach") of the partner agency's procedures or of the Sacramento CoC privacy and security plan the user will be sanctioned accordingly. HMIS end users, partner agencies, or HMIS Administrator must report potential violations of any privacy and security protocols ("data breach") described in the partner agency's procedures or of the Sacramento CoC privacy and security plan.

The responsibilities include:

- HMIS end users are obligated to report suspected data breach instances to the partner agency's administrator or the HMIS Administrator as soon as possible.
- The Partner Agency's Security personnel or HMIS Administrator will investigate.
- HMIS end users found to be in violation will be sanctioned accordingly. Sanction may include but are not limited to suspension of the HMIS system access and/or revocation of the HMIS system privileges.

In the broadest sense, data breach includes acts related to crime (but not limited to):

- Blackmail to demand for money or other consideration under threat to do bodily harm, to injure property, to accuse of a crime, or to expose secrets.
- Fraud as an intentional deception made for personal gain or to damage another individual.
- Identity theft.
- Improper use of your user ID and password such as sharing or giving another person your User ID and password for HMIS access, selecting the option to have browsers save your HMIS password.
- Release client PPI to any other organization without proper client consent except as provided by federal and California State law.
- Stalking &/or attempt to stalk.

Policy and Procedures – Reporting Instances

1. Any HMIS end user who becomes aware of or suspects a data breach instance has been compromised must immediately report the concern to their Partner Agency Security personnel. The HMIS Administrator will temporarily suspend the HMIS end user access until the completion of an internal investigation. The internal investigation shall be conducted as soon as possible and must not exceed thirty (30) days. An email notification of the temporary suspension will be provided to the HMIS end user and the partner agency.
    a. After the completion of the internal investigation and it is determined a data breach instance then the Partner Agency Security personnel will report that to the HMIS Administrator.

OR

Any HMIS Administrator who becomes aware of or suspects a data breach instance has been compromised, identifies a system breach, privacy breach, security breach, misuse of the

system, or unethical use of the system, the HMIS Administrator must immediately report the concern. The HMIS Administrator will temporarily suspend the HMIS end user access until the completion of an investigation. The investigation shall be conducted as soon as possible and must not exceed thirty (30) days. An email notification of the temporary suspension will be provided to the HMIS end user and the partner agency.

2. Upon receiving notice of an end user suspected data breach instance, the HMIS Administrator will investigate to determine validity.
    a. If the HMIS Administrator need assistance with the investigation, the partner agency may be requested to help. This may include a request to provide documentation of the HMIS end user misuse or unethical use of the system, substantiated incidents that may have compromised HMIS system security and/or client privacy whether or not a release of client PPI is definitively known to have occurred.
    b. When the HMIS Administrator need assistance from the partner agency the request will be emailed detailing the specifics of the request and the timeframe for delivering their findings. The timeframe to respond to the request is within five (5) business days.
3. The HMIS Administrator will complete a report that must be signed by the HMIS Lead Agency Programs Director and the HMIS Manager [Attachment A: Initial Investigation Report].
4. If the HMIS Administrator investigation concludes that the HMIS end user did not acted out of accordance with the Sacramento CoC Privacy & Security Plan, their HMIS access will resume. An email notification regarding the temporary suspension will be provided to the HMIS end user and the partner agency.
5. If the HMIS Administrator investigation concludes that the HMIS end user acted out of accordance and unlawfully, the incident will be escalated to the designated HMIS & Data Committee (HDC) members. The HMIS Administrators and the HDC members will collectively review the incident [Attachment B: Secondary Investigation Report] to determine the outcome of the HMIS end user access. The HMIS Administrator will ensure the HMIS end user identifying information and employment with the partner agency is not release and will remain anonymous.
    a. If there is a conflict of interest, the designated HDC member(s) will be withdrawn from reviewing the incident.
    b. For each suspected instance 3 HDC members will volunteer to be part of the review panel. The designated members will be contacted on an as-needed basis.

The HMIS Administrator should be notified of any substantiated 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.

Reactivating and Reinstating

The HMIS System Administrator reserves the right to permanently deactivate the former HMIS end user access. In consideration of reactivating and reinstating the HMIS end user access:

1. The former HMIS end user must submit in writing to the HMIS System Administrator to request for reactivating and/or reinstating HMIS access.
2. The HMIS Administrators and the HDC members will collectively review the previous Investigation Report(s) as to the reason(s) and action(s) that prompted the HMIS end user access to be terminated.
3. The HMIS Administrators and the HDC members will collectively determine the severity of the

HMIS end user's action and the length of time that has passed.

4. The HMIS Administrator and HDC members will need the HMIS end user to provide written acknowledgment of understanding of the reasoning of the breach and be remorseful of the action.

The decision to reactivate and reinstate the HMIS end user access will be documented and justified. The HMIS Lead Agency Programs Director, HMIS Manager, and HDC members will sign the Notice of Clearance [Attachment C: Notice of Clearance].

The decision to not reactivate and reinstate the HMIS end user access will be documented and justified. The HMIS Lead Agency Programs Director, HMIS Manager, and HDC members will sign the Notice of Refusal [Attachment D: Notice of Refusal].

The HMIS Administrator will ensure the HMIS end user identifying information and employment with the partner agency is not release and will remain anonymous.

a. If there is a conflict of interest, the designated HDC member(s) will be withdrawn from reviewing the incident.
b. For each reactivation and reinstatement request, 3 HDC members will volunteer to be part of the review panel. The designated members will be contacted on an as-needed basis.

Attachment A – Initial Investigation Report

INITIAL INVESTIGATION REPORT

The HMIS System Administrator has completed the investigation regarding the [date] allegation of [*breach/misuse/unethical conduct; describe the information you have including dates, etc*].

We hereby have determined to not terminate [Name] HMIS access for the following reason(s):

- Misuse by…
- Unethical conduct….

Description/Reason

The [Name] shall receive a copy of this Investigation Report within five (5) business days.

The Partner Agency shall receive a copy of this Investigation Report within five (5) business days.

_____ _____

Signature of HMIS Lead Agency Programs Director Date

_____ _____

Signature of HMIS System Administrator, HMIS Manager Date

Attachment B – Secondary Investigation Report

SECONDARY INVESTIGATION REPORT

The HMIS System Administrator and members of the HMIS & Data Committee (HDC) have completed the investigation regarding the [date] allegation of [*breach/misuse/unethical conduct; describe the information you have including dates, etc*].

We hereby have determined to terminate [Name] HMIS access for the following reason(s):

- Misuse by…
- Unethical conduct….

Description/Reason

The [Name] shall receive a copy of this Investigation Report within five (5) business days.

The Partner Agency shall receive a copy of this Investigation Report within five (5) business days.

_____ _____

Signature of HMIS Lead Agency Programs Director Date

_____ _____

Signature of HMIS System Administrator, HMIS Manager Date

_____ _____

Signature the HMIS & Data (HDC) designated Committee Member Date

_____ _____

Signature the HMIS & Data (HDC) designated Committee Member Date

_____ _____

Signature the HMIS & Data (HDC) designated Committee Member

Date

Attachment C – Notice of Clearance

NOTICE OF CLEARANCE

On [date], [Name] applied for HMIS access. Pursuant to the HMIS Department Investigation Report [date], [Name] HMIS access was previously terminated due to (breach/misuse/unethical conduct). Accordingly, HMIS Department and the HMIS & Data (HDC) committee members are granting you access, but unable to provide you with further information.

You, [Name] shall receive a copy of this Notice of Clearance of reactivating and reinstating HMIS access within five (5) business days.

The current partner agency you are employed with shall receive a copy of this Notice of Clearance of reactivating and reinstating HMIS access within five (5) business days.

The Partner Agency shall receive a copy of this Investigation Report within five (5) business days.

_____ _____

Signature of HMIS Lead Agency Programs Director

Date

_____ _____

Signature of HMIS System Administrator, HMIS Manager

Date

_____ _____

Signature the HMIS & Data (HDC) designated Committee Member

Date

_____ _____

Signature the HMIS & Data (HDC) designated Committee Member

Date

_____ _____

Signature the HMIS & Data (HDC) designated Committee Member

Date

Attachment D – Notice of Refusal

NOTICE OF REFUSAL

On [date], [Name] applied for HMIS access. Pursuant to the HMIS Department Investigation Report [date], [Name] HMIS access was previously terminated due to (breach/misuse/unethical conduct). Accordingly, HMIS Department and the HMIS & Data (HDC) committee members are denying you access, but unable to provide you with further access to HMIS.

You, [Name] shall receive a copy of this Notice of Refusal of reactivating and reinstating HMIS access within five (5) business days.

The current partner agency you are employed with shall receive a copy of this Notice of Refusal of reactivating and reinstating HMIS access within five (5) business days.

The Partner Agency shall receive a copy of this Investigation Report within five (5) business days.

_____ _____

Signature of HMIS Lead Agency Programs Director Date

_____ _____

Signature of HMIS System Administrator, HMIS Manager Date

_____ _____

Signature the HMIS & Data (HDC) designated Committee Member Date

_____ _____

Signature the HMIS & Data (HDC) designated Committee Member Date

_____ _____

Signature the HMIS & Data (HDC) designated Committee Member Date

Document History

Date of Revision	Document Version #	Revision Notes
MM/DD/YYYY	1.0	First Release of Document
MM/DD/YYYY	1.1	…. CoC Board Approval