HMIS PRIVACY & SECURITY PLAN

Sacramento County 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 (November 14, 2018)

Contents

Introduction

The HMIS Lead Agency is responsible for overseeing HMIS privacy and security. The HMIS Lead Agency may delegate some specific duties related to maintaining HMIS privacy and security to an 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. 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 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 semiannually.

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 (69 Federal Register 45888) 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 and for the agencies which participate in an HMIS. This section describes the Privacy Plan of the Sacramento County HMIS System. We intend our policy and plan to be consistent with the HUD standards. All users, 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 are truly a client of the Sacramento County Continuum of Care. 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 which 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 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 collects, utilizes and discloses information.	*REQUIRED* Agencies must adopt a privacy statement which meets all minimum standards. It is strongly recommended to post this Statement on your Agency's local website (if available).
Consumer Notice Posting: 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 Posting.
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 to 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 users and direct service providers protect and maintain their privacy. The role and responsibilities of the user cannot be over-emphasized. A user is defined as a person that has direct interaction with a client or their data. (This could potentially be any person at the agency: staff member, volunteer, contractor, 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

Agency Responsibilities

The 2004 HUD HMIS Standards emphasize that it is the agency's responsibility for upholding client privacy. All 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 agency may exceed the minimum standards described and are encouraged to do so. Agencies must have an adopted Privacy Statement which meets the minimum standards before data entry into the HMIS can occur.

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 (69 Federal Register 45888)
- 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, the agency must 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 includes name, Social Security Number (SSN), date of birth, zip code, project entry and/or exit date, and unique personal identification number (HMIS Unique Identifier).

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 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, law enforcement 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 uses 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 your 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. 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 a quiz on HMIS procedures annually. Users who fail to score 70% or above on the quiz will be required to 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 and revised in March 2010. 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 Sacramento County HMIS Lead Agency, using the contact information below.

All questions and requests related to this Privacy Statement should be directed to: Tina Wilton with Sacramento Steps Forward: twilton@sacstepsforward.org or 916.993-7707.

HMIS Lead Agency: System Administration 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 users upholding system privacy.
- Monitor agencies to ensure adherence to their adopted Privacy Plan.
- Develop action and compliance plans for agencies that do not have adequate Privacy Statements.
- Maintain the HMIS Website to keep all references within the Baseline Privacy Statement up to date.
- Provide training to agencies and users on this Privacy Plan.
- Remove all personally identifiable information from user accounts after they have been inactive for 7 years. This PII may be stored in a secure location to enable the system administrator re-identify records if the need arises.

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 system administrators, 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 (69 Federal Register 45888) 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. 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 agency may exceed the minimum standards described in this plan and are encouraged to do so. All 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 agencies must apply the security standards addressed in this Security Plan to all the systems where personal protected information is stored or accessed. Additionally, all security standards must be applied to all networked devises. This includes, but is not limited to, networks, desktops, laptops, mobile devises, mainframes and servers.

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 a reasonable amount of time to address any concerns. Egregious violations of the security plan may result in immediate termination of an agency or user's access to the HMIS as determined by the HMIS Lead.

Security Officer

The HMIS Lead Agency will designate a Lead Security Officer 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.

Lead Security Officer

- May be an HMIS System Administrator or another employee, volunteer or contractor designated by the HMIS Lead Agency who has completed HMIS training 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 Agency,
- Reviews and maintains file of Partner Agency annual compliance certification checklists,
- Conducts security audit of all Partner Agencies, on an as needed basis.

Partner Agency

- Conducts a security audit for any workstation that will be used for HMIS purposes,
  - No less than annually for all agency HMIS workstations, AND
  - Prior to issuing 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 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 forwards the Checklist to the Lead Security Officer.

Upon request, the HMIS Lead Agency may be available to provide Security support 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 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 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. A remote wipe and/or remote disable option should also be downloaded onto the device.

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.
- 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). End-Users will 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.
- Partner Agency 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).
- Partner Agency 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 HMIS System Administrator, in conjunction with the Partner Agency Security Officer, 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 Officer is responsible for ensuring that all agency End Users have completed a 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 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 verbally in person.
- When the Partner Agency 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 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 consecutive unsuccessful attempts to login will disable the User ID until the password is reset. For Agency End Users, passwords should 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 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. The HMIS System Administrator will attempt to contact the Partner Agency 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 Partner Agency 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 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.
- 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.
- The Continuum of Care is empowered to permanently revoke a Partner Agency's access to HMIS for substantiated noncompliance with the provisions of these Security Standards, the

Sacramento County HMIS Policies and Procedures, or the HMIS Privacy Statement that resulted in a release of PPI.

Disposing Electronic, Hardcopies, Etc.

- Computer: All technology equipment (including computers, printers, copiers and fax machines) used to access HMIS and which will no longer be used to access HMIS will 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.
- 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

- The Lead Security Officer shall develop and implement procedures for managing new, retired, and compromised HMIS account credentials.
- The Partner Agency Security Officer shall develop and implement procedures for managing new, retired, and compromised local system account credentials.
- The Partner Agency Security Officer 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.
- SSF will make a HIPPA compliant cloud file storage solution available. Agencies should leave all documents containing PPI on that file storage site.

Disaster Recovery Plan

Disaster recovery for the Sacramento County 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

Sacramento has a shared HMIS system providing HMIS Users with access to client's current or past history from other agencies. Agencies have sought to hire individuals with lived experience of homelessness or who are currently experiencing homelessness. These 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 provided additional training on the restrictions on the use of HMIS data.

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 managing the HMIS be subject to a criminal background check. 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. 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 results of the background check must be retained in the employee's personnel file.

Partner Agency 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 Partner Agency.
- Criminal background checks must be completed on all new End Users, and the "Background Check Review and Verification Statement" on the New User Request Form must be signed by the HR Department. The New User Request Form must be submitted to the local Lead Agency System Administrator prior to End Users gaining access to the HMIS.

HMIS Lead Procedure

The HMIS Lead 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 SSF, 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 should not be given access to the HMIS. The Partner Agency's HR Department must only sign the Background Check Review and Verification Statement if 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 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.

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 that HMIS system security and/or client privacy has been compromised must immediately report the concern to their Partner Agency Security Officer.
- In the event of a suspected security or privacy concern the Partner Agency Security Officer should 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 Partner Agency Security Officer should have the HMIS System Administrator deactivate the End

User's User ID until the internal investigation has been completed.

- Following the internal investigation, the Partner Agency Security Officer shall notify the Lead Security Officer of any 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. If the security or privacy concern resulted from demonstrated noncompliance by an End User with the HMIS End User Agreement, the Lead Security Officer reserves the right to permanently deactivate the User ID for the End User in question.
- Within one business day after the Lead Security Officer receives notice of the security or privacy concern, the Lead Security Officer and Partner Agency 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 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 County 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.
- In the event of a substantiated release of PPI in noncompliance with the provisions of these Security Standards, the Sacramento County HMIS Policies and Procedures, or the Partner Agency Privacy Statement, the Partner Agency Security Officer will make a reasonable attempt to notify all impacted individual(s). The Lead Security Officer must approve of the method of notification and the Partner Agency Security Officer must provide the Lead Security Officer with evidence of the Agency's notification attempt(s). If the Lead Security Officer is not satisfied with the Agency's efforts to notify impacted individuals, the Lead Security Officer will attempt to notify impacted individuals at the Agency's expense.
- The HMIS Lead Agency will notify the appropriate body of the Continuum of Care 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.
- The HMIS Lead Agency will maintain a record of all substantiated releases of PPI in noncompliance with the provisions of these Security Standards, the Sacramento County HMIS Policies and Procedures, or the Partner Agency Privacy Statement for 7 years.
- The Continuum of Care 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 County HMIS Policies and Procedures, or the Partner Agency Privacy Statement that resulted in a release of PPI.

Privacy and Security Monitoring

New HMIS Partner Agency Site Security Assessment

- Prior to establishing access to HMIS for a new Partner Agency, the Lead Security Officer will assess the security measures in place at the Partner Agency to protect client data (see Technical Safeguards – Workstation Security). The Lead Security Officer or other HMIS System Administrator will meet with the Partner Agency Executive Director (or executive-level designee) and Partner Agency Security Officer to review the Partner Agency's information security protocols prior to countersigning the HMIS Memorandum of Understanding. 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 HMIS Agency Security Officer.

Semiannual Partner Agency Self-Audits

- The Partner Agency Security Officer will use the Compliance Certification Checklist to conduct semiannually security audits of all Partner Agency HMIS End User workstations.
- The Partner Agency 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 (i.e.: personal computer) that is not subject to the Partner Agency Security Officer's regular audits.
- If areas are identified that require action due to noncompliance with these standards or any element of the Sacramento County HMIS Policies and Procedures, the Partner Agency Security Officer will note these on the Checklist, and the Partner Agency Security Officer and/or HMIS Agency Administrator will work to resolve the action item(s) within 15 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. The findings, action items, and resolution summary must be reviewed and signed by the Agency's Executive Director or other empowered officer prior to being forwarded to the Lead Security Officer.
- The Partner Agency Security Officer must turn in a copy of the Checklist to the Lead Security Officer on a semiannual basis.

Annual Security Audits

- The Lead Security Officer will schedule the annual security audit in advance with the Partner Agency Security Officer.
- The Lead Security Officer will use the Compliance Certification Checklist to conduct security audits.
- The Lead Security Officer must randomly audit at least 10% of the workstations used for HMIS data entry for each HMIS Partner Agency. In the event that an agency has more than 1 project site, at least 1 workstation per project site must be audited.
- If areas are identified that require action due to noncompliance with these standards or any element of the Sacramento County HMIS Policies and Procedures, the Lead Security Officer will note these on the Checklist, and the Partner Agency Security Officer and/or HMIS Agency Administrator will work to resolve the action item(s) within 15 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 other empowered officer and forwarded to the HMIS Lead Security Officer.