Santa Barbara County HMIS
Data Security Plan

Continuum of Care:

CA-603 Santa Maria/Santa Barbara County

HMIS Lead Agency:

County of Santa Barbara
Community Services Department
Housing and Community Development Division
105 E. Anapamu St., Room 105
Santa Barbara, CA 93101
Telephone: (805) 568-3520
Fax: (805) 560-1091

Contents

1. Introduction

This document indicates the techniques and procedures that will be used to protect the security of clients and other people who contribute information to the Homeless Management Information System (HMIS) for the Santa Maria/Santa Barbara County Continuum of Care.

As described in the March 2010 HMIS Data Standards Revised Notice, an HMIS is an electronic data collection system that stores longitudinal person-level information about persons who access the homeless services system in a Continuum of Care. HMIS is a valuable resource because of its capacity to integrate and unduplicate data from all homeless assistance and homeless prevention programs in a Continuum of Care. Aggregate HMIS data can be used to understand the size, characteristics and needs of the homeless population at the local, state and national levels. The HMIS Data and Technical Standards are issued by the U.S. Department of Housing and Urban Development (HUD).

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

- 2004 HMIS Data and Technical Standards Final Notice
- Guidance on HPRP Subgrantee Data Collection and Reporting for Victim Service Providers
- 2011 HMIS Requirements Proposed Rule
- 2017 HMIS Data Standards Revised Notice

The roles and responsibilities described in this document will primarily be fulfilled by the Continuum of Care, the HMIS Lead Agency, and HMIS Partner Agencies (referred to by HUD as Contributing Homeless Organizations or CHOs).

A Continuum of Care is a group composed of representatives of organizations, including nonprofit providers of homeless services, faith-based organizations, governments, businesses, advocates, public housing agencies, school districts, social service providers, veterans service providers, mental health agencies, hospitals, universities, affordable housing developers and law enforcement, that serve homeless and formerly homeless persons and that carry out the responsibilities delegated to a Continuum of Care under HUD’s regulations for a particular community. A Continuum of Care is ultimately responsible for oversight and guidance of HMIS. A Continuum of Care is also responsible for oversight of the security of the data and any public use of the data.

The Director of the Community Services Department, or his/her designee, is the authorizing agent for all agreements made between HMIS Partner Agencies and the HMIS Lead Agency. In all HMIS governance decisions, the Continuum of Care will balance the interests and needs of all HMIS stakeholders, including homeless men, women and children, service providers, and policy makers.

The HMIS Lead Agency provides day-to-day management of system participation, operations and security. In Santa Barbara County, the role of HMIS Lead Agency is currently filled by the Housing and Community Development Division of the Community Services Department of the County of Santa Barbara.

An HMIS Partner Agency is an entity that has agreed to uphold these Policies and Procedures by executing a Memorandum of Understanding with the County of Santa Barbara. Some HMIS Partner Agencies may be obligated to comply with the Health Insurance Portability and Accountability Act (“HIPPA”), and/or with 42 CFR Part 2, regarding the confidentiality of substance use disorder patient records. Where possible, these agencies should comply with HIPAA, with 42 CFR Part 2, and with this Privacy Plan. If it is not possible to reconcile all of the applicable rules, then agencies should comply with the more stringent regulations. Agencies and programs are responsible for ensuring HIPAA and 42 CFR Part 2 compliance.

2. Revision History

These Policies and Procedures and Security Plan shall be reviewed and, if necessary, revised at least annually by the Continuum of Care. See Section 6.6 of the Administrative Policies and Procedures for more detail on changes of this and other documents.

Date	Author	Description
11/30/2013	Community Technology Alliance (www.CTAgroup.org)	Full revision referencing all HUD standards and 2011 HEARTH HMIS Proposed Rule
4/14/2014	County of Santa Barbara Community Services Department	Revisions referencing designations
10/20/2017	HomeBase	Technical revisions based on best practices in other communities. Security Plan split off from general Policies and Procedures, and established as stand-alone document.

3. Security Procedures

3.1 Technical Administrators

Policies

- Each HMIS Partner Agency must have at least one active, trained Technical Administrator at all times. A Partner Agency with 10 or more active HMIS licenses should also designate a trained Deputy Technical Administrator who can assist the Technical Administrator with his or her duties on an as-needed basis.
- The Partner Agency Technical Administrator is responsible for preventing degradation of the HMIS resulting from viruses, intrusion, or other factors within the agency's control.
- The Partner Agency Technical Administrator is responsible for preventing inadvertent release of confidential client-specific information through physical, electronic or visual access to the workstation.
- Each Partner Agency is responsible for ensuring they meet the Privacy and Security requirements detailed in the HUD HMIS Data and Technical Standards.

Procedures

1. Each Partner Agency shall designate a primary contact for communications regarding HMIS by submitting a Partner Agency Technical Administrator Agreement signed by the Technical Administrator and the Partner Agency's Executive Director to the HMIS Lead Agency. The authorizing agent of the HMIS Lead Agency will countersign the Partner Agency Technical Administrator Agreement. The HMIS Lead Agency will return a copy of the countersigned Partner Agency Technical Administrator Agreement to the Partner Agency's Technical Administrator.
2. The Partner Agency may designate a new or replacement primary contact in the same manner as above.
3. The HMIS Lead Agency will maintain a file of all signed Partner Agency Technical Administrator Agreement forms and make it available upon request to HMIS End Users or to the Continuum of Care.
4. Technical Administrators must complete the appropriate training in security, privacy, and data quality at least once per year. If any of these trainings are conducted remotely, then it is the Technical Administrator's responsibility to transmit proof of completing the training to the HMIS Lead in a timely fashion.
5. If all of a Partner Agency's Technical Administrators are all unable to perform their duties due to illness, travel, leave, insufficient training, etc., then the Partner Agency must designate a new Technical Administrator within 30 calendar days.
6. In the event a Partner Agency is unwilling or unable to designate a qualified Technical Administrator, the HMIS Lead Agency reserves the right to recover from the Partner Agency any costs associated with the HMIS Lead Agency carrying out these responsibilities on behalf of the Partner Agency.

3.2 Physical Access Restrictions

ACCESSING HMIS FROM A DESKTOP OR LAPTOP

- To protect the security of HMIS data, computers that are used to access HMIS must be physically located inside a secure facility, such as an office set aside for the use of Partner Agency staff. Laptops may be taken into and out of these areas, but laptops may not be used to access HMIS while the laptop is outside of a secure facility.
- HMIS End User must log out of HMIS when finished using HMIS.

- Workstations automatically turn on a password protected screen saver when the workstation is temporarily not in use.
- HMIS may not be accessed from computers that are placed in mixed-use areas that are accessible to clients, casual volunteers, or visitors.
- Non-authorized persons should not be able to see an HMIS workstation screen without breaching a physical barrier such as a desk or a fence.
- The Partner Agency's Technical Administrator will monitor the IP addresses used to log into HMIS to ensure that End Users are complying with these controls.
- The owner, authorized user, model, and serial number of each laptop that is used to access HMIS must be written down and on file with an Agency's Technical Administrator before the device is used to access HMIS. (Desktops do not need to be registered because they are rarely lost or stolen).
- Documents printed from HMIS must be sent only to printers in secure locations. All printed documents must be promptly collected and securely stored by an End User who will take responsibility for the printed materials. The printed materials must be destroyed (e.g., shredded) as soon as they are no longer needed, and the printer must be checked at least once daily to identify and dispose of any unclaimed documents.

ACCESSING HMIS FROM A PHONE OR TABLET

- Only outreach workers may use mobile devices such as phones or tablets to access HMIS.
- The owner, authorized user, model, and serial number of each mobile device that is used to access HMIS must be written down and on file with an Agency's Technical Administrator before the device is used to access HMIS.
- HMIS End Users must log out of HMIS when finished using HMIS.
- Mobile devices that are used to access HMIS must not store or "memorize" HMIS-related passwords; users should be required to re-enter their password from scratch each time they log on.
- Whenever possible, mobile devices that are used to access HMIS should be registered for remote detection and remote wiping, so that a lost or stolen device can be located and/or reset to factory settings.
- No outreach worker may register more than one mobile device at a time for HMIS access. Each such device must be configured to lock its screen after no more than 60 seconds of inactivity and protected with a unique, robust password.

3.3 Workforce Access Restrictions

Each participating agency must conduct a criminal background check on each of its Technical Administrators at its own expense. The results of the criminal background checks will be shared with the HMIS Lead System Administrator.

1. The HMIS Lead Agency must consider the results of the background check on a case-by-case basis, with the goal of protecting the security and integrity of the HMIS system and safeguarding the personal information contained therein.
2. An individual whose background raises concerns about whether s/he may sufficiently be relied upon to help the HMIS Lead Agency achieve this goal may not be given administrative-level access to HMIS.
3. An individual whose background raises concerns about whether s/he may sufficiently be relied upon to help the HMIS Lead Agency achieve this goal may be enrolled as an HMIS End User. After at least one year, if the individual demonstrates through proper and safe use of HMIS that the individual is reliable and trustworthy, then the individual may apply to become a Technical Administrator. At least once during the first year in which the individual is licensed as an End User, the agency's Technical Administrator should generate a report on the times, places, accounts, and terminals used by the End User to log in, transfer or edit data, and print files generated by HMIS. If, in the process of

generating these reports, the Technical Administrator identifies any areas of concern, the Technical Administrator will promptly share the relevant report with the HMIS Lead so that they can discuss whether it is appropriate to continue licensing the new End User.

4. The results of the background check must be retained in the subject's personnel file by the Technical Administrator.
5. Background check may be conducted only once for each person unless otherwise required.

3.4 Electronic Access Restrictions

Workstation Security

1. Each Partner Agency is responsible for obtaining hardware, software, and internet connectivity that meets or exceeds HUD requirements and HMIS Vendor specifications. Use of technology infrastructure that is not compliant with the standards and requirements may pose a security risk and could result in slow performance.
2. The HMIS Lead Agency will pursue the use of PKI (Public Key Infrastructure) 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). The Partner Agency Technical Administrator will ensure that a current PKI certificate (available from the HMIS Lead Agency) has been installed on each End User's workstation.
3. Partner Agency Technical Administrator will confirm that at a minimum, 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).
4. Partner Agency Technical Administrator will confirm that any workstation accessing HMIS has and uses a hardware or software firewall.
5. HMIS End Users should use caution when connecting to HMIS via wireless Internet. HMIS may never be accessed via unsecured wireless internet (e.g. public network, no password). At least one security protocol (such as WEP) must be used at all times when accessing HMIS on wireless Internet.
6. The Partner Agency Technical Administrator shall develop and implement other procedures as needed to prevent unauthorized users from connecting to private agency networks.

Establishing HMIS User IDs and Access Levels

1. The Partner Agency Technical Administrator will ensure that any prospective End User reads, understands and signs the HMIS End User Agreement.
2. The Partner Agency Technical Administrator is responsible for ensuring that all agency End Users have completed mandatory trainings, including HMIS Security and Privacy training and End User Responsibilities and Workflow training, prior to being provided with a User ID to access HMIS.
3. The Partner Agency Technical Administrator will maintain a file of all signed HMIS End User Agreements.
4. The HMIS Lead Agency will maintain a file of all signed Partner Agency Technical Administrator Agreements.
5. All End Users will be issued a unique User ID and password. Sharing of User ID and password 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. Although the HMIS Lead Agency may transfer an HMIS license from one Partner Agency employee to another, User IDs and passwords may not be transferred from one user to another. Instead, the HMIS Lead Agency shall issue a new User ID and a new Password each time an HMIS license is transferred.
6. The Partner Agency Technical Administrator will always attempt to assign the most restrictive access that allows the End User to efficiently and effectively perform his/her assigned duties.
7. The HMIS Lead Agency will create the new user ID and notify the user ID owner of the temporary password verbally via telephone or in person.

8. When the Partner Agency Technical Administrator determines that it is necessary to change a user's access level, the HMIS Lead Agency will update the user ID as needed.

Passwords

1. Temporary passwords must be changed on first use. User-specified passwords must be a minimum of 8 characters long and must contain a combination of letters and at least two numbers.
2. End Users will be prompted by the software to change their password at least every 45 days.
3. End Users must immediately notify their Partner Agency Security Officer if they have reason to believe that someone else has gained access to their password.
4. Three consecutive unsuccessful attempts to login will disable the User ID until the password is reset. For Agency End Users and Technical Administrators), passwords shall be reset by the HMIS Lead Agency.

Rescinding User Access

1. Partner Agencies shall notify the HMIS Lead Agency within 24 hours if an End User's access should be terminated because the End User no longer requiring access to HMIS due to changes in job duties, termination of employment, or any other reason.
2. The HMIS Lead Agency reserves the right to terminate End User licenses that are inactive for 90 days or more. The HMIS Lead Agency will attempt to contact the Partner Agency Technical Administrator for the End User in question prior to termination of the inactive user license.
3. 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 Technical Administrator shall notify the HMIS Lead Agency. The HMIS Lead Agency reserves the right to deactivate User IDs pending further investigation if an End User's noncompliance with the HMIS End User Agreement is suspected or demonstrated. The Partner Agency Technical Administrator shall notify the HMIS Lead Agency 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).
4. The Continuum of Care is empowered to permanently revoke End User access to HMIS for a breach of security or confidentiality.

3.5 Backups and Archives

Backups – HMIS Lead

The HMIS Lead Agency will maintain appropriate backups of HMIS Data in collaboration with the HMIS Vendor so as to preserve the ability to restore the system to any of at least three different "save points." All backups will be protected with appropriate passwords and encryption and kept in a secure location.

Backups – Partner Agencies

In the course of their work, Partner Agencies may desire to archive, export, print, or otherwise make copies of HMIS Data. To maintain security, Partner Agencies may never print, copy, e-mail, or otherwise transmit protected personal information ("PPI"). PPI includes names, birthdates, Social Security numbers, and other information that could be used to personally identify a particular client.

Instead of copying PPI, Partner Agencies must either view PPI within the HMIS software on an approved terminal, or copy de-identified information into a new file or document, without copying the PPI. Even when information has been de-identified, agencies should still use caution when copying or printing HMIS data, and should print only as needed for specific work-related tasks.

3.6 Damage Control

Reporting Security Incidents

These Security Standards and the associated Santa Barbara County 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.

1. Any HMIS End User who becomes aware of or suspects a breach of HMIS system security and/or client privacy must immediately report that breach to the Partner Agency Technical Administrator.
2. In the event of a breach resulting from suspected or demonstrated noncompliance by an End User with the HMIS End User Agreement, the Partner Agency Technical Administrator should deactivate the End User's User ID until an internal agency investigation has been completed.
3. Following an internal investigation, the Partner Agency Technical Administrator shall notify the HMIS Lead Agency of any substantiated incidents that may have resulted in a breach of HMIS system security and/or client privacy (whether or not a breach is definitively known to have occurred). If the breach resulted from suspected or demonstrated noncompliance by an End User with the HMIS End User Agreement, the HMIS Lead Agency reserves the right to deactivate the User ID for the End User in question pending further investigation.
4. Within 1 business day after the HMIS Lead Agency receives notice of the breach, the HMIS Lead Agency and Partner Agency Technical Administrator will jointly establish an action plan to analyze the source of the breach and actively prevent future breaches. The action plan shall be implemented as soon as possible, and the total term of the plan must not exceed 30-days.
5. If the Partner Agency is not able to meet the terms of the action plan within the time allotted, the HMIS Lead Agency may elect to terminate the Partner Agency's access to HMIS. The Partner Agency may appeal to the appropriate body of the Continuum of Care for reinstatement to HMIS following completion of the requirements of the action plan.
6. In the event of a substantiated breach of client privacy through a release of PPI in noncompliance with the provisions of these Security Standards, the Santa Barbara County HMIS Policies and Procedures, HMIS End User Agreement, or any other HMIS plans, forms, standards, or governance documents, the Partner Agency Technical Administrator will attempt to notify any impacted individual(s).
7. 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 Santa Barbara County HMIS Policies and Procedures, HMIS End User Agreement, or any other HMIS plans, forms, standards, or governance documents.
8. The HMIS Lead Agency will maintain a record of all substantiated releases of PPI in noncompliance with the provisions of these Security Standards, the Santa Barbara County HMIS Policies and Procedures, HMIS End User Agreement, or any other HMIS plans, forms, standards, or governance documents for 7 years.
9. The Continuum of Care reserves the right to permanently revoke a Partner Agency's access to HMIS for a breach of security or privacy.

Disaster Recovery Plan

Disaster Recovery for the Santa Barbara County HMIS will be conducted by the HMIS software vendor. However, the HMIS Lead Agency must be familiar with the disaster recovery plan set in place by the HMIS software vendor.

1. The HMIS Lead Agency should maintain ready access to the following information:
    i. Contact information – Phone number and email address of the Bowman Systems contact responsible for the agency's data after a disaster.
    ii. Agency responsibilities – A thorough understanding of the agency's role in facilitating recovery from a disaster.
2. All HMIS Lead Agency personnel should be aware of and trained to complete any tasks or procedures for which they are responsible in the event of a disaster.
3. The HMIS Lead Agency must have a plan for restoring local computing capabilities and internet connectivity for the HMIS Lead Agency's facilities. This plan should include the following provisions.
    i. Account information – Account numbers and contact information for internet service provider, support contracts, and equipment warranties.
    ii. 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.
    iii. Network and system configuration information – Documentation of the configuration settings required to restore local user accounts and Internet access.

3.7 Security Audits

Initial Site Security Assessment

Prior to establishing access to HMIS for a new Partner Agency, the HMIS Lead Agency will assess the security measures in place at the Partner Agency to protect client data. A representative of the HMIS Lead Agency will meet with the Partner Agency Executive Director (or executive-level designee) and Partner Agency Technical Administrator to review the Partner Agency’s information security protocols prior to countersigning the Memorandum of Understanding. This 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 Technical Administrator.

Ongoing Monitoring by Technical Administrator

1. The Partner Agency Technical Administrator must conduct a security audit for any workstation that will be used for HMIS data collection or entry
    ii. no less than quarterly for all agency HMIS workstations, AND
    iii. prior to issuing a User ID to a new HMIS End User, AND,
    iv. any time an existing user moves to a new workstation.
2. The Partner Agency Security Officer must continually ensure each workstation within the Partner Agency used for HMIS data collection or entry is adequately protected by a firewall and antivirus software.

Quarterly Partner Agency Self-Audit

1. In any agency with at least three active HMIS licenses, the Partner Agency Technical Administrator will use the Compliance Certification Checklist to conduct quarterly security audits of all Partner Agency End User workstations. In an agency with two or fewer active HMIS licenses that had no security non-compliance issues in the previous calendar year, the Security Officer may instead use an informal method to assure that all Partner Agency End User workstations are secure.
2. The Partner Agency Technical Administrator will audit remote access by associating User IDs, IP addresses and login date/times with employee time sheets. End Users may not remotely access HMIS from a workstation (i.e.: personal computer) that is not subject to the Partner Technical Administrator’s regular audits.
3. If areas are identified that require action due to noncompliance with these Security Standards, the Santa Barbara County HMIS Policies and Procedures, HMIS End User Agreement, or any other HMIS

plans, forms, standards, or governance documents, the Partner Agency Technical Administrator will note these on the Compliance Certification Checklist, and the Partner Agency Technical Administrator will work to resolve the action item(s) within 30 days.

4. Any Compliance Certification Checklist that includes 1 or more findings of noncompliance and/or action items will not be considered valid until all action items have been resolved. The Checklist findings, action items, and resolution summary must be reviewed and signed by the Partner Agency Executive Director or other empowered officer prior to being returned to the HMIS Lead Agency.
5. The Partner Agency Technical Administrator must turn in a copy of the Compliance Certification Checklist to the HMIS Lead Agency on a quarterly basis.

Annual Comprehensive Security Audit by HMIS Lead

1. The HMIS Lead Agency will schedule the annual comprehensive security audit in advance with the Partner Agency Technical Administrator.
2. The HMIS Lead Agency will use the Compliance Certification Checklist to conduct security audits.
3. The HMIS Lead Agency must randomly audit at least 10% of the workstations for each HMIS Partner Agency, rounded up to the nearest whole workstation. In the event that an agency has more than 1 program site, at least 1 workstation per program site must be audited.
4. One Compliance Certification Checklist must be filled out per audited workstation.
5. If areas are identified that require action due to noncompliance with these these Security Standards, the Santa Barbara County HMIS Policies and Procedures, HMIS End User Agreement, or any other HMIS plans, forms, standards, or governance documents, the HMIS Lead Agency will note these on the Compliance Certification Checklist, and the Partner Agency Technical Administrator will work to resolve the action item(s) within 30 days.
6. Any Compliance Certification Checklist that includes 1 or more findings of noncompliance and/or action items will not be considered valid until all action items have been resolved and the Checklist findings, action items, and resolution summary has been reviewed and signed by the Partner Agency Executive Director or other empowered officer and returned to the HMIS Lead Agency.

4. Forms Control

All forms required by these Policies and Procedures are available in on the HMIS web portal. Completed forms must be filed as described in the chart below and maintained for 7 years.

Filing of Completed Forms

Form ID #	**Form title**	**Responsibility for maintaining file of signed forms**
1MOU-20171020	Memorandum of Understanding	HMIS Lead Agency
1CC-20171020	Compliance Certification Checklist	HMIS Lead Agency
1EU-20171020	HMIS End User Agreement	Partner Agency Technical Administrator
1ROI-20171020	Client Informed Consent and Release of Information Authorization	Partner Agency End User
1SI-20171020	Standardized Intake	N/A

Form ID Syntax: Version Number + Form Code – YYYYMMDD of last revision