Santa Barbara County HMIS Policies & Procedures and 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
123 E. Anapamu St., Second Floor
Santa Barbara, CA 93101
Telephone: (805) 568-3520
Fax: (805) 560-1091

Contents

1. Introduction

This document provides the framework for the ongoing operations of 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
- 2010 HMIS Data Standards Revised Notice
- 2011 HMIS Requirements Proposed Rule

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.

In Santa Barbara County, the Central Coast Collaborative on Homelessness (C3H) serves as the Continuum of Care. 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.

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. All HMIS End Users are required to read and comply with the HMIS Data and Technical Standards. Failure to comply with the HUD standards carries the same consequences as failure to comply with these Policies and Procedures. In any

instance where these Policies and Procedures and Security Plan are not consistent with the HUD HMIS Standards, the HUD Standards take precedence. Should any inconsistencies be identified, please immediately notify the HMIS Lead Agency.

For agencies or programs where HIPAA applies, HIPAA requirements take precedence over both the HUD HMIS Data Requirements (as specified in those requirements) and these Policies and Procedures. Agencies and programs are responsible for ensuring HIPAA compliance.

The Project Overview provides the main objectives, direction and benefits of HMIS. Governing Principles establish the values that are the basis for all policy statements and subsequent decisions. Operating Procedures provides specific policies and steps necessary to control the operational environment and enforce compliance in project participation, workstation security, user authorization and passwords, collection and entry of client data, release and disclosure of client data, training, compliance, and technical support. The Other Obligations and Agreements section discusses additional considerations of this project and the Forms Control section provides information on obtaining forms, filing and record keeping.

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 6.10 for Policies and Procedures related to 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

3. Project Overview

The long-term vision of HMIS is to enhance Partner Agencies' collaboration, service delivery and data collection capabilities by sharing information. Accurate information will put the Continuum of Care in a better position to request funding from various sources and help plan better for future needs. HMIS is designed to be an integrated network of homeless and other service providers that use a central database to collect, track and report uniform information on client needs and services. This system will not only meet Federal requirements but also enhance service planning and delivery.

A fundamental goal of HMIS is to document the demographics of homelessness in Santa Barbara County according to the HUD HMIS directive. It is the goal of the Continuum of Care to achieve an accurate count of the number of community residents experiencing homelessness, identify patterns in the utilization of assistance, and document the effectiveness of the services for the client. This will be accomplished through analysis of data that is gathered from people experiencing homelessness and the service providers who assist them in shelters and homeless assistance programs throughout the county. Data that is gathered via intake interviews and program participation will be used to complete HUD Annual Performance Reports, Annual Homeless Assessment Reports, and point-in-time shelter counts. This data may also be analyzed to provide unduplicated counts and anonymous aggregate data to policy makers, service providers, advocates, and consumer representatives.

The local HMIS project utilizes a web-enabled application residing on a central server to facilitate data collection by homeless service organizations across the county. Access to HMIS is limited to agencies who have agreed to uphold these Policies and Procedures by executing a Memorandum of Understanding with the HMIS Lead Agency, and then only to authorized staff members who meet the necessary training and security requirements.

Homeless individuals and case managers can benefit from HMIS as a result of improved service coordination. HMIS facilitates information sharing among case management staff within one agency or between agencies (with written client consent) who are serving the same clients.

Agencies serving homeless individuals and program managers can benefit from HMIS by obtaining access to aggregate information that can be used to develop a more complete understanding of clients' needs and outcomes. Such information can then be used to advocate for additional resources, to conduct evaluations of program services, and to report to funding agencies such as HUD.

The Continuum of Care and policy makers can benefit from HMIS because county-wide use of a single shared data collection system provides the capacity to generate the HUD Annual Homeless Assessment Report and allows access to aggregate information that will assist in identification of gaps in services, as well as the completion of other service reports used to inform policy decisions aimed at addressing and ending homelessness at local, state and federal levels.

4. Governing Principles

It is the primary governing principle of the Santa Barbara County HMIS that HMIS is intended to serve and protect the community's clients. As such,

- Clients will be understood to be the owners of their own data. Each individual will have the right to grant informed consent, limit data sharing, or revoke consent related to his/her PPI at any time.
- Security and confidentiality will be the top priorities of all End Users, who will serve as stewards of their clients' data.
- All End Users will strive for the highest possible degree of data quality. Data quality is a social justice issue because poor data quality can lead to reductions in funding and services, clients not being referred to the appropriate services to meet their needs, or improper findings of ineligibility.
- The community will use HMIS to improve service coordination and outcomes through data-driven decision making.
- The community will encourage broad HMIS participation by human services agencies.

HMIS End Users are expected to read, understand, and adhere to the spirit of these principles, even when the Policies and Procedures do not provide specific direction.

5. Roles and Responsibilities

The Continuum of Care is responsible for:

- HMIS management and administration in compliance with all applicable regulations,
- Designating a single information system as the official HMIS software for the region,
- Designating an HMIS Lead Agency,
- Executing an HMIS governance charter and maintaining documentation of compliance with that charter,
- Reviewing, revising and approving all HMIS plans, forms, standards and governance documents,
- Developing and implementing a strategic plan for HMIS participation, development and use in data-driven decision making,
- Authorizing the release of aggregate system-wide data on homelessness within the Continuum of Care at least annually,
- Confirming the resolution of security breaches,
- Using HMIS data to identify gaps in services to the homeless and promote solutions to local policy makers,
- Promoting and/or enforcing HMIS participation,
- Ensuring sufficient HMIS funding,
- Educating and raising consciousness of the community about homelessness.

The HMIS Lead Agency is responsible for:

- Liaising with HUD regarding federal HMIS standards and regulations,
- Developing HMIS plans, forms, standards and governance documents in compliance with all applicable regulations,
- Executing and maintaining copies of signed Memoranda of Understanding with Partner Agencies,
- Monitoring and providing regular reports to the Continuum of Care regarding HMIS data and Partner Agencies' compliance with local HMIS plans, forms, standards and governance documents,
- Liaising with HMIS software vendor(s),
- Procuring HMIS software and licenses,
- Overseeing software license administration, including adding and removing Partner Agency Technical Administrators,
- Configuring HMIS software to meet Continuum of Care and/or Partner Agency needs ,
- Maintaining HMIS web portal and resource library, including domain registration,
- Ensuring sound configuration of network and security layers,
- Ensuring the performance of system backup and disaster recovery processes,
- Developing and presenting training curriculum on the following topics: ethics/confidentiality, new user orientation, program management, agency technical administration, specialized applications and custom reporting,
- Maintaining documentation of training attendance,
- Providing End User help desk support,
- Completing aggregate data reporting and extraction on behalf of the Continuum of Care, including Annual Performance Reports (APRs), Annual Homeless Assessment Report (AHAR), and Annual Sheltered Point-in-Time Counts,
- Applying for funding from HUD,

The Partner Agency is responsible for:

- Signing and complying with the Memorandum of Understanding and all applicable plans, forms, standards and governance documents,

- Conducting a thorough annual review of internal compliance with all applicable HMIS plans, standards and governance documents,
- Detecting and responding to violations of any applicable HMIS plans, standards and governance documents,
- Completing thorough and accurate data collection as specified by HMIS forms and standards,
- Monitoring and maintaining security of all staff workstations used for HMIS data entry,
- Ensuring End User adherence to workstation security policies,
- Safeguarding client privacy through compliance with confidentiality and security policies,
- Securing and maintaining documentation of client informed consent,
- Designating a Partner Agency Technical Administrator to provide first-level End User support,
- Managing End User licenses,
- Ensuring all agency End Users complete the User Agreement and maintaining documentation of all User Agreements,
- Ensuring all agency End Users complete mandatory training and forwarding documentation of training provided by an authorized Partner Agency Technical Administrator to the HMIS Lead Agency,
- Providing and maintaining workstations with internet connectivity,
- Maintaining agency and program descriptor data in HMIS,
- Completing agency-level HUD reporting,
- Performing authorized imports of client data.

Ombudsperson

The _____ will serve as the Ombudsperson for HMIS-related disputes. While every participant in the system, including clients, should have access to the Ombudsperson, reasonable efforts should be made (and documented if possible) to obtain satisfaction by other means, including escalation within an agency and through the HMIS Lead Agency.

6. Operating Procedures

6.1 Project Participation

Policies

- Agencies participating in HMIS shall commit to abide by the governing principles of HMIS and adhere to the terms and conditions of this partnership as detailed in the Memorandum of Understanding.

Procedures

Site Security Assessment

1. 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 (see section 5.2 Workstation Security). A representative of the HMIS Lead Agency will meet with the Partner Agency Executive Director (or executive-level designee) and Partner Agency Technical Administrator/Security Officer 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/Security Officer.

Confirm Participation

1. The Partner Agency shall confirm its participation in HMIS and commitment to these Policies and Procedures by submitting a Memorandum of Understanding signed by the Partner Agency's Executive Director to the HMIS Lead Agency. The authorizing agent of the HMIS Lead Agency will countersign the Memorandum of Understanding. The HMIS Lead Agency will return a copy of the countersigned Memorandum of Understanding to the Partner Agency's Technical Administrator.
2. The HMIS Lead Agency will maintain a file of all signed Memorandums of Understanding.
3. Each Partner Agency shall re-confirm the agency's participation in HMIS and commitment to these Policies and Procedures at least annually by submitting a Memorandum of Understanding signed by the Partner Agency's Executive Director to the HMIS Lead Agency. The authorizing agent of the HMIS Lead Agency will countersign the Memorandum of Understanding. The HMIS Lead Agency will return a copy of the countersigned Memorandum of Understanding to the Partner Agency's Technical Administrator.
4. The HMIS Lead Agency will maintain and publicly publish a list of all current Partner Agencies on the HMIS web portal.

Assign Technical Administrator

1. Each Partner Agency shall designate a primary contact for communications regarding HMIS by submitting a Partner Agency Technical Administrator Agreement signed by 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.

4. The HMIS Lead Agency will maintain a list of all assigned Partner Agency Technical Administrators and make it available upon request to HMIS End Users or to the Continuum of Care.
5. 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.

Voluntary Termination of Participation

1. The Partner Agency shall inform the HMIS Lead Agency in writing of their intention to terminate their participation in HMIS.
2. The HMIS Lead Agency will remove the departing agency from the list of Partner Agencies on the HMIS web portal.
3. The HMIS Lead Agency will revoke access of the Partner Agency staff to HMIS. Note: All Partner Agency information contained in the HMIS system will remain in the HMIS system.
4. The HMIS Lead Agency will keep all termination records on file with the associated Memorandums of Understanding.
5. The agency will be responsible for any cost of obtaining a hard copy or digital copy of HMIS information.

Termination of Participation for Lack of Compliance

1. When the HMIS Lead Agency determines that a Partner Agency is in violation of the Memorandum of Understanding by not fully complying with HMIS plans, forms, standards and/or governance documents, the HMIS Lead Agency will work directly with the Partner Agency's Executive Director to resolve the issue(s) in question.
2. If the HMIS Lead Agency and Partner Agency are unable to resolve issue(s), the Ombudsperson will be called upon to resolve the issue(s). If that results in a ruling of termination:
    i. The Partner Agency will be notified in writing by the Ombudsperson of the intention to terminate the agency's participation in HMIS.
    ii. The HMIS Lead Agency will revoke access of the Partner Agency staff to HMIS. Note: All Partner Agency information contained in the HMIS system will remain in the HMIS system.
    iii. The HMIS Lead Agency will keep all termination records on file with the associated Memorandums of Understanding.
    iv. Following the involuntary termination, the Partner Agency may appeal to the Ombudsperson for reinstatement to HMIS provided the Partner Agency has corrected the issue(s) resulting in the initial termination ruling.
    v. The Continuum of Care is empowered to permanently revoke a Partner Agency's access to HMIS for a serious and/or willful breach of security or confidentiality.

6.2 Security

Policies

- The Partner Agency Security Officer is responsible for preventing degradation of the HMIS resulting from viruses, intrusion, or other factors within the agency's control.
- The Partner Agency Security 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. Partner Agencies will conduct a thorough review of internal policies and procedures regarding HMIS quarterly.
- To promote the security of HMIS and the confidentiality of the data contained therein, access to HMIS will be available only through approved workstations.

Procedures

Security Officers

The HMIS Lead Agency and all HMIS Partner Agencies must designate Security Officers to oversee HMIS privacy and security.

Lead Security Officer

1. HMIS Lead Agency System Administrator
2. Assesses security measures in place prior to establishing access to HMIS for a new Partner Agency,
3. Reviews and maintains file of Partner Agency annual compliance certification checklists,
4. Conducts annual comprehensive security audit of all Partner Agencies.

Partner Agency Security Officer

1. May be the Partner Agency Technical Administrator,
2. Conducts a security audit for any workstation that will be used for HMIS data collection or entry
    i. no less than quarterly for all agency HMIS workstations, AND
    ii. prior to issuing a User ID to a new HMIS End User, AND,
    iii. any time an existing user moves to a new workstation.
3. 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),
4. Completes the Quarterly Compliance Certification Checklist, and forwards the Checklist to the HMIS Lead Agency.

Security Audit

New HMIS Partner Agency Site Security Assessment

1. 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 (see Technical Safeguards – Workstation Security). A representative of the HMIS Lead Agency will meet with the Partner Agency Executive Director (or executive-level designee) and Partner Agency Technical Administrator/Security Officer 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/Security Officer.

Quarterly Partner Agency Self-Audits

1. The Partner Agency Security Officer will use the Compliance Certification Checklist to conduct quarterly security audits of all Partner Agency End User workstations.
2. The Partner Agency Security Officer 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 (ie: personal computer) that is not subject to the Partner Agency Security Officer's regular audits.
3. If areas are identified that require action due to noncompliance with these standards or any element of the Santa Barbara County HMIS Policies and Procedures, the Partner Agency Security Officer will note these on the Compliance Certification Checklist, and the Partner Agency Security Officer and/or Technical Administrator will work to resolve the action item(s) within one month.
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 Security Officer must turn in a copy of the Compliance Certification Checklist to the HMIS Lead Agency on a quarterly basis.

Annual Comprehensive Security Audits

1. The Lead Security Officer will schedule the annual comprehensive security audit in advance with the Partner Agency Security Officer.
2. The Lead Security Officer will use the Compliance Certification Checklist to conduct security audits.
3. The Lead Security Officer must randomly audit at least 10% of the workstations for each HMIS Partner Agency. 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 standards or any element of the Santa Barbara County HMIS Policies and Procedures, the Lead Security Officer will note these on the Compliance Certification Checklist, and the Partner Agency Security Officer and/or Technical Administrator will work to resolve the action item(s) within one month.
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.

Physical Safeguards

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

1. Computer Location – Computer must be in a secure location where only authorized persons have access. Computer must not be accessible to clients, the public or other unauthorized Partner Agency staff members or volunteers.
2. Printer location – Documents printed from HMIS must be sent to a printer in a secure location where only authorized persons have access.
3. 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.

Technical Safeguards

Workstation Security

1. The HMIS Lead Agency will enlist 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 Security Officer will ensure that a current PKI certificate (available from the HMIS Lead Agency) has been installed on each End User's workstation.
2. Partner Agency Security Officer 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).
3. Partner Agency Security Officer will confirm that any workstation accessing HMIS has and uses a hardware or software firewall.

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 Ethics/Confidentiality training and End User Responsibilities and Workflow training, prior to being provided with a User ID to access HMIS. See section 5.6 Training.
3. The Partner Agency Technical Administrator will maintain a file of all signed HMIS End User Agreements.
4. 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. User IDs and passwords may not be transferred from one user to another.
5. 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.
6. The Partner Agency Technical Administrator will create the new user ID and notify the user ID owner of the temporary password verbally via telephone or in person.
7. When the Partner Agency Technical Administrator determines that it is necessary to change a user's access level, the Partner Agency Technical Administrator 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 every 45 days.
3. End Users must immediately notify their Partner Agency Technical Administrator 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 (not including Partner Agency Technical Administrators), passwords should be reset by the Partner Agency Technical Administrator, but in some cases may be reset by the HMIS Lead Agency. For Partner Agency Technical Administrators, passwords may only be reset by the HMIS Lead Agency.

Other Technical Safeguards

Most other technical safeguards for the Santa Barbara County HMIS are currently implemented by the HMIS software vendor. However, Security Officers are responsible for appropriately managing passwords and other account information that could allow unauthorized individuals access to HMIS data.

1. The Lead Security Officer shall develop and implement procedures for managing new, retired, and compromised HMIS account credentials.
2. The Partner Agency Security Officer/Technical Administrator shall develop and implement procedures for managing new, retired, and compromised local system account credentials.
3. The Partner Agency Security Officer/Technical Administrator shall develop and implement procedures that will prevent unauthorized users from connecting to private agency networks.
4. 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 "Recycle Bin" emptied before the End User leaves the workstation.

Workforce Security

The HMIS Lead Agency must conduct a background check on any individual to be designated as a Lead Security Officer and/or 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. An individual whose background indicates that s/he may not sufficiently be relied upon to help the HMIS Lead Agency achieve this goal may not be given administrative-level access to HMIS.
2. The results of the background check must be retained in the subject's personnel file.
3. Background check may be conducted only once for each person unless otherwise required.

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 Security Officer.
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 Security Officer should deactivate the End User's User ID until an internal agency investigation has been completed.
3. Following an internal investigation, the Partner Agency Security Officer shall notify the Lead Security Officer 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 Lead Security Officer reserves the right to deactivate the User ID for the End User in question pending further investigation.
4. Within 1 business day after the Lead Security Officer receives notice of the breach, the Lead Security Officer and Partner Agency Security Officer 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, in consultation with the Ombudsperson, may elect to terminate the Partner Agency's access to HMIS. The Partner Agency may appeal to the Ombudsperson 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, or the Partner Agency Privacy Statement, the Lead Security Officer 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, or the Partner Agency Privacy Statement.
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, or the Partner Agency Privacy Statement 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 Lead Security Officer 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.

6.3 User Authorization & Password Security

Policies

- End Users shall commit to abide by the governing principles of HMIS and adhere to the terms and conditions of the HMIS End User Agreement.
- An appropriate level of HMIS access will be provided to those individuals that require access to perform their assigned duties on behalf of an HMIS Partner Agency.
- 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.

Procedures

1. User authorization and password security is established by the Security Standards. A Partner Agency's adoption of these Policies and Procedures will constitute acknowledgement of the responsibilities of the Partner Agency as defined in the associated Security Standards.

Rescinding User Access

1. End User access should be terminated by the Partner Agency Technical Administrator within 24 hours if an End User no longer requires access to perform their assigned duties due to a change of job duties or termination of employment.
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/Security Officer should deactivate the User ID for the End User in question until an internal agency investigation has been completed. The Partner Agency Technical Administrator/Security Officer shall notify the HMIS Lead Agency 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).

4. In the event the Partner Agency Technical Administrator is unable or unwilling to do so, the HMIS Lead Agency also 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.
5. The Continuum of Care is empowered to permanently revoke End User access to HMIS for a breach of security or confidentiality.

6.4 Collection and Entry of Client Data

Policies

- Client data will be gathered according to the policies, procedures and confidentiality rules of each individual program.
- Client data may only be entered or imported into HMIS if the client has provided informed consent, as demonstrated by a signed HMIS Client Informed Consent and Release of Information Authorization form.
- Victim service providers may not directly enter or provide client-level data to HMIS.
- Each Partner Agency is responsible for collecting and entering all of the elements on the Standardized Intake Form, whether or not they are required to do so by their funding source.
- The Partner Agency that creates a client record owns the responsibility for a baseline of data quality to include: non-duplication of the client record, Client Informed Consent and Release of Information Authorization (ROI), Universal & Program Level Data Elements as defined by HUD Data Standards, and Program Entries and Exits. Quality assurance shall be the ultimate responsibility of each Partner Agency's Executive Director.
- All HMIS Partner Agencies shall be committed to timely, accurate and complete entry of client-specific data into HMIS in order to provide program managers and local policy makers with reports that facilitate strategic planning.

Procedures

1. The HMIS Lead Agency will maintain a resource library on the HMIS web portal that includes at minimum the community's Standardized Intake Form, HMIS Client Informed Consent and Release of Information Authorization (ROI), HMIS End User Manual and Data Quality Plan. When any of these items is updated, the HMIS Lead Agency will attempt to notify all current End Users of the change.
2. End Users' data collection and data entry practices should follow the workflow and specific data entry guidelines established in the Standardized Intake Form, HMIS Client Informed Consent and Release of Information Authorization (ROI), HMIS End User Manual, Data Quality Plan and/or training materials available on the HMIS web portal resource library. It is the End User's responsibility to ensure that s/he is always using the current versions of these forms and resources.
3. Victim service providers, defined as a private nonprofit organization whose primary mission is to provide services to victims of domestic violence, dating violence, sexual assault or stalking, must use a comparable database that collects client-level data over time and generates unduplicated aggregate reports based on the data. Legal service providers may also elect to use a comparable database if it is necessary to protect attorney-client privileges.
4. Client data will be entered into HMIS as soon possible following intake or service start date (not more than 3 business days later).
5. Any authorized data imports will be the responsibility of the Partner Agency.
6. The Partner Agency Technical Administrator is responsible for monitoring agency data quality on a weekly basis and forwarding error logs to agency End Users for correction. The HMIS Lead Agency will provide training to the Partner Agency Technical Administrator on how to access data quality reports and how to support End Users in correcting errors.

7. The Continuum of Care will adopt a plan to dispose of (or remove identifiers from) client data 7 years after it was created or last changed. Once adopted, that plan will be incorporated into these Policies and Procedures.

6.5 Release and Disclosure of Client Data

Policies

- Client-specific data from HMIS may be shared with Partner Agencies only when the sharing agency has secured informed consent authorizing such sharing, as demonstrated by a signed HMIS Client Informed Consent and Release of Information Authorization form, and only during such time that Client Informed Consent and Release of Information Authorization is valid (before its expiration). Other non-HMIS inter-agency agreements do not cover the sharing of HMIS data. Sharing of client data may be limited by program specific confidentiality rules.
- No client-specific data will be released or shared outside of the Partner Agencies unless the client gives specific written permission or unless withholding that information would be illegal. Note that services may NOT be denied if client refuses to sign Client Informed Consent and Release of Information Authorization or declines to state any information.
- Aggregate data that does not contain any client-specific identifying data may be shared with internal and external agents without specific permission. This policy should be made clear to clients as part of the Informed Consent procedure.
- A client shall have the right to receive a copy of all HMIS data relating to him/her upon written request.
- Each Partner Agency Executive Director is responsible for his or her agency's internal compliance with these standards.

Procedures

1. Client Informed Consent and Release of Information Authorization (ROI) must constitute informed consent. The burden rests with the Partner Agency End User or intake counselor to inform the client about the purpose and function of HMIS data before asking for consent. As part of informed consent, a notice must be posted in the intake area explaining the reasons for collecting the data, the client's rights with regard to data collection, and any potential future uses of the data. An example of such a sign may be found in the HMIS web portal resource library.
2. Partner Agency End Users must obtain a new signed ROI and enter it into HMIS if the client's original release has expired.
3. Upon written request to the HMIS Lead Agency, a client shall be given a print-out of all data relating to him/her within 10 working days.
4. Upon written request to the HMIS Lead Agency, a report of data sharing events, including dates, agencies, persons, and other details, must be made available to a client within 10 working days.
5. A log of all external releases or disclosures of PPI must be maintained by the HMIS Lead Agency for 7 years and made available to the client upon written request and within 10 working days.
6. If a client signs an ROI, but chooses not to share information with other Partner Agencies, End Users' data collection and data entry practices should follow the workflow and specific data entry guidelines established in the HMIS End User Manual to prevent sharing of client assessment information.
7. End Users or Partner Agency Technical Administrators will not share client-specific HMIS data with any person who is not also a current HMIS End User.

6.6 Training

Policies

- The HMIS Lead Agency is responsible for developing an HMIS training curriculum and materials and for providing ongoing trainings at sufficient intervals to promote high levels of data quality and consistent compliance with HMIS plans, forms, standards and governance documents.
- The Partner Agency Technical Administrator is responsible for ensuring that all agency End Users have completed mandatory trainings prior to being provided with a User ID to access HMIS.

Procedures

1. The HMIS Lead Agency will develop and maintain curriculum and training materials on the following topics:
    i. HMIS Security and Privacy training
    ii. Partner Agency Technical Administrator responsibilities and workflow training
    iii. Partner Agency Technical Administrator 'train-the-trainer' training
    iv. End User responsibilities and workflow training
    v. Data quality training
    vi. Module-specific training
    vii. Program management, HMIS oversight and basic reporting training
    viii. Advanced Reporting Tool (ART) basic training
2. The HMIS Lead Agency will be responsible for providing any trainings related to significant changes or updates in the HMIS software or system configuration. If the software changes are significant enough to warrant mandatory retraining of all users, the HMIS Lead Agency will attempt to notify all End Users of available training opportunities and to inform End Users of any applicable consequences of failure to attend mandatory training.
3. The HMIS Lead will maintain training records for 7 years.
4. All End Users must complete Security and Privacy training annually.
5. All End Users must complete a refresher version of End User responsibilities and workflow training annually.
6. All Partner Agency Technical Administrators must complete a refresher version of Partner Agency Technical Administrator responsibilities and workflow training annually in addition to completing End User responsibilities and workflow training annually.
7. A Partner Agency Technical Administrator who has attended 'train-the-trainer' training may be authorized by the HMIS Lead Agency to conduct some trainings for End Users. Attendance records and documentation of attendees' comprehension of the presented material (if applicable) must be forwarded by the Partner Agency Technical Administrator to the HMIS Lead Agency within 1 business day of a training hosted by a Partner Agency Technical Administrator.

Training

All new HMIS End Users must complete Security and Privacy training prior to accessing HMIS and annually thereafter. Partner Agencies are encouraged to have additional non-HMIS employees and volunteers complete Security and Privacy training during orientation and annually thereafter to ensure that all individuals interacting with clients and using agency workstations are upholding these Security Standards. The HMIS Lead Agency will maintain training records for 7 years.

6.7 System Administration

Policies

- The HMIS Lead Agency, in partnership with the software vendor, will strive to maintain continuous system availability by design and by practice.

Procedures

1. The HMIS Lead Agency will inform End Users in advance of any planned interruptions in service.

6.8 Compliance

Policies

- Using reports available through the HMIS software, all changes to client data will be periodically and randomly audited for compliance.

Procedures

1. The HMIS Lead Agency will provide standard data quality, performance measurement, and compliance monitoring reports to the Continuum of Care at regular intervals to be established by the Continuum of Care. It is the responsibility of each Partner Agency to be aware of these reporting intervals and to ensure that the agency's data is current and accurate. Copies of reports submitted to the Continuum of Care will be made available to Partner Agencies by the HMIS Lead Agency.
2. The HMIS Lead Agency will complete all required annual reports to HUD on behalf of the Continuum of Care.
3. The HMIS Lead Agency will monitor all HUD communications regarding HMIS and update the Continuum of Care and Partner Agencies as appropriate about new standards, open comment periods, and/or recommendations.
4. As necessary, the HMIS Lead Agency will make recommendations to the appropriate Continuum of Care body regarding proposed changes to HMIS plans, forms, standards and governance documents as a result of changes to HUD standards or community practices.

6.9 Technical Support

Policies

- End Users submit support requests to their Partner Agency Technical Administrator, who may escalate the request to the HMIS Lead Agency, who may in turn escalate the request to the HMIS software vendor as appropriate. Support requests include reporting problems, requests for feature enhancements, or other general technical support. Under no circumstances should End Users submit support requests directly to the HMIS software vendor.
- The HMIS Lead Agency will only provide support for issues specific to HMIS software and systems.

Procedures

1. If an End User encounters a problem or originates an idea for improvement to the HMIS system configuration or software, that End User should send a request via email to the Partner Agency Technical Administrator specifying the severity of the problem, its impact on the End User's work, specific information necessary to reproduce the problem (browser information, client ID#, date/time stamping, etc.), and any other documentation that might facilitate the resolution of the problem. The requesting End User should also provide his/her contact information and best times to contact.
2. The Partner Agency Technical Administrator, upon receipt of a support request, shall make reasonable attempts to resolve the issue.
3. If the Partner Agency Technical Administrator is unable to resolve the issue and determines that the problem is specific to the HMIS software and/or system configuration, the Partner Agency Technical Administrator shall consolidate multiple similar requests and submit a support request to the HMIS Lead Agency via email.

4. If the support request is deemed by HMIS Lead Agency to be an agency-specific customization, resolution of the request may be prioritized accordingly. Upon the agreement of both parties, the HMIS Lead Agency reserves the right to charge a Partner Agency on an hourly basis for agency-specific customizations. Agency-specific customizations may include, but are not limited to, new assessments, new data fields, and new options in drop-down menus.
5. If the HMIS Lead Agency determines that the cause of a reported issue is outside the scope of control of the HMIS Lead Agency's System Administrator, the HMIS Lead Agency may forward the request to the HMIS software vendor, or contract with other software or technical support providers as necessary to resolve the issue(s).
6. Requests from funders and/or jurisdictions for aggregate agency- or program-level data should be directed to the appropriate Partner Agency Technical Administrator (or other agency contact person) with the information provided directly to the requesting jurisdiction by that Partner Agency.

6.10 Changes to This and Other Documents

Policies

- All plans, forms, standards and governance documents regulating the operation and administration of the Santa Barbara County HMIS shall be reviewed and, if necessary, revised at least annually by the Continuum of Care.
- The HMIS Lead Agency will be responsible for notifying the Continuum of Care if an update to one or more of the plans, forms, standards and governance documents is necessary.

Procedures

Changes to Policies & Procedures

1. Proposed changes to HMIS plans, forms, standards and governance documents may originate from any Continuum of Care member.
2. When proposed changes originate within an HMIS Partner Agency, they must be reviewed by the Partner Agency Executive Director, and then submitted by the Partner Agency Executive Director to the HMIS Lead Agency.
3. HMIS Lead Agency will maintain a list of proposed changes.
4. The list of proposed changes will be reviewed and discussed at least annually by the Continuum of Care, or a designated committee of the Continuum of Care. The date and time of this discussion will be communicated to all Continuum of Care members and HMIS End Users through established Continuum of Care communication channels.
5. Recommended changes to HMIS plans, forms, standards and governance documents resulting from the review and discussion of proposed changes by the Continuum of Care or Continuum of Care committee will be forwarded to the Continuum of Care Board for approval.
6. Within 10 working days after approval by the Continuum of Care Board, the HMIS Lead Agency will forward a copy of the adopted HMIS plans, forms, standards and/or governance documents to all HMIS Partner Agency Executive Directors. Partner Agency Executive Directors shall acknowledge receipt and acceptance of the adopted HMIS plans, forms, standards and/or governance documents in writing or by email to HMIS Lead Agency within a subsequent 10 working days. The Partner Agency Executive Director shall also circulate the revised document to all End Users within his/her agency and ensure agency compliance with the adopted HMIS plans, forms, standards and/or governance documents.

7. Other Obligations and Agreements

Policy

- Current funding for HMIS provides for a limited number of software End User licenses. While it may not be possible to meet every Partner Agency's requests for End User licenses within the existing funding, the HMIS Lead Agency, in partnership with the Continuum of Care, will endeavor to ensure that every Partner Agency will have its minimum requirements met.

Procedure

1. The HMIS Lead Agency, with approval from the Continuum of Care, may establish a reasonable fee structure for Partner Agencies to participate in HMIS. Partner agencies will be given an opportunity to provide feedback on any proposed fee structure before it is adopted. If adopted, the fee structure will be incorporated into the HMIS Governance Charter and Partner Agency Memorandum of Understanding. The fee structure implementation plan will provide Partner Agencies with sufficient time before the first fee payment is due to allow Partner Agencies to attempt to secure additional funding to cover the expense.

8. 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-20131130	Memorandum of Understanding	HMIS Lead Agency
1TA-20131130	Partner Agency Technical Administrator / Security Officer Agreement	HMIS Lead Agency
1CC-20131130	Compliance Certification Checklist	HMIS Lead Agency
1EU-20131130	HMIS End User Agreement	Partner Agency Technical Administrator
1ROI-20131130	Client Informed Consent and Release of Information Authorization	Partner Agency End User
_____	Standardized Intake	Partner Agency End User

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