HMIS MOSBE Security Plan

Adopted by the Monterey and San Benito Continuum of Care X/XX/2014

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 Officer 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 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 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.
- 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

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. May be an HMIS System Administrator or another employee, volunteer or contractor designated by the HMIS Lead Agency who has completed HMIS Privacy and Security training and is adequately skilled to assess HMIS security compliance,
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 security audit of all Partner Agencies.

Partner Agency Security Officer

1. May be the Partner Agency Technical Administrator or another Partner Agency employee, volunteer or contractor who has completed HMIS Privacy and Security training and is adequately skilled to assess HMIS security compliance,
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 Lead Security Officer.

Security Audit

New HMIS Partner Agency Site Security Assessment

1. 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), Partner Agency HMIS Technical Administrator 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 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 HMIS 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 Monterey and San Benito Counties 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 HMIS 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 forwarded to the Lead Security Officer.
5. The Partner Agency Security Officer must turn in a copy of the Compliance Certification Checklist to the Lead Security Officer on a quarterly basis.

Annual Security Audits

1. The Lead Security Officer will schedule the annual 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. Each compliance check for each computer should be noted in the compliance Checklist.
5. If areas are identified that require action due to noncompliance with these standards or any element of the Monterey and San Benito Counties 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 forwarded to the HMIS Lead Security Officer.

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 – A computer used as an HMIS workstation must be in a secure location where only authorized persons have access. The HMIS workstation 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 System Administrator) has been installed on each End User's workstation.
2. 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).
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 Privacy, Security and Ethics 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. 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.
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 user account as necessary.

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 System Administrator. For Partner Agency Technical Administrators, passwords may only be reset by the HMIS System Administrator.

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 his or her assigned duties due to a change of job duties or termination of employment.
2. The HMIS System Administrator reserves the right to terminate End User licenses that are inactive for 90 days or more. The HMIS System Administrator 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 should deactivate the User ID for the End User in question until an internal agency investigation has been completed. The Partner Agency Technical Administrator or Partner Agency 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 System Administrator is empowered 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 a Partner Agency's access to HMIS for substantiated noncompliance with the provisions of these Security Standards, the Monterey and San Benito Counties HMIS Policies and Procedures, or the Partner Agency Privacy Statement that resulted in a release of Personal Protected Information (PPI).

Other Technical Safeguards

Most other technical safeguards for the Monterey and San Benito Counties HMIS are currently implemented by the HMIS software vendor.

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 shall develop and implement procedures for managing new, retired, and compromised local system account credentials.
3. The Partner Agency Security Officer 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 "Recycling Bin" emptied before the End User leaves the workstation.

Workforce Security

The HMIS Lead Agency will ensure background checks are conducted on any individual to be designated as a Lead Security Officer and/or HMIS System Administrator.

1. The results of the background check must be considered 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 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. A background check may be conducted only once for each person unless otherwise required.

Reporting Security Incidents

These Security Standards and the associated Monterey and San Benito Counties 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 compromise of HMIS system security and/or client privacy must immediately report that possible incident to the Partner Agency Security Officer.
2. In the event of a suspected security compromise the Partner Agency Security Officer should complete an internal investigation. If the suspected compromise resulted from an End User's suspected or demonstrated noncompliance with the HMIS End User Agreement, the Partner Agency Security Officer should deactivate the End User's User ID until the internal investigation has been completed.
3. Following the 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 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.
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 System Administrator, in consultation with the Monterey and San Benito Counties Continuum of Care 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 Personal Protected Information (PPI) in noncompliance with the provisions of these Security Standards, the Monterey and San Benito Counties HMIS Policies and Procedures, or the Partner Agency Privacy Statement, the Agency 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 Personal Protected Information (PPI) in noncompliance with the provisions of these Security Standards, the Monterey San Benito Counties HMIS Policies and Procedures, or the Partner Agency Privacy Statement.
8. The HMIS Lead Agency will maintain a record of all substantiated releases of Personal Protected Information (PPI) in noncompliance with the provisions of these Security Standards, the Monterey and San Benito Counties 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 substantiated noncompliance with the provisions of these Security Standards, the Monterey and San Benito Counties HMIS Policies and Procedures, or the Partner Agency Privacy Statement that resulted in a release of Personal Protected Information (PPI).

Disaster Recovery Plan

Disaster Recovery for the Monterey and San Benito Counties HMIS will be conducted by the HMIS software Administrator CTA . In collaboration with the HMIS vendor Bowman Systems

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 recovering 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 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.
3. 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.
    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.