Pima County

Homeless Management Information System

(HMIS)

Security Plan

Approved August 26, 2014

HMIS SECURITY PLAN

The goal of the HMIS Security Plan is to ensure that HMIS data is collected, used, and maintained in a confidential and secure environment at all times. The HMIS Security Plan applies to the HMIS Lead/Administrator, HMIS participating agencies, and the HMIS Bowman software. These standards apply to all client information that is collected in the HMIS or through comparable databases.

The purpose of this document is to outline security standards and define the parameters of compliance with these standards. These standards represent a minimum level of security required for all HMIS participating agencies.
Another key purpose of this document is to describe how the HMIS Lead/Administrator and HMIS vendor software meet and maintain security requirements established in HUD's security standards.

LEVELS OF USER ACCESS AND SECURITY

Each HMIS Participating Agency will maintain a written policy detailing organizational management control over access authorization, user levels, and the internal process for activating new HMIS users. The HMIS Administrator will be solely responsible for establishing new users in the HMIS.

HMIS Participating Agencies must establish an internal point of contact, known as the Agency Administrator, for establishing new users with the HMIS Administrator. Individual staff should not email or request new HMIS users or HMIS program changes without permission from the Agency Administrator. Directors should be copied on the correspondence so that they are aware of new user requests.

The Pima County HMIS has four levels of user types:

1) ***Volunteer* –**HMIS users are assigned to programs at an agency to view and modify client records and can be assigned 'Enter Data As' rights for programs outside of their agency.

2) ***Agency Staff* –** HMIS users are assigned to programs at an agency to view and modify client records, can be assigned 'Enter Data As' rights for programs outside of their agency and update their agency's 'system news'.

3) ***Case Manager II*–** HMIS users are assigned to program at an agency to view and modify client records and goals/action steps, can be assigned 'Enter Data As' rights for programs outside of their agency, and update their agency's 'system news'. This user can also access the Call Point module, modify case managers, and run agency reports.

4) ***Case Manager III*–** HMIS users are assigned to program at an agency to view and modify client records and goals/action steps, can be assigned 'Enter Data As' rights for programs outside of their agency, and update their agency's 'system news'. This user can also access the Call Point module, modify case managers, and run agency reports. This user has an 'agency administrator' view of all programs within their agency.

An agency must identify the both the type of user and programs each user should access within their agency. The Agency Administrator must maintain listings of active users and notify the HMIS Administrator immediately (within 24 hours) of any HMIS users that are no longer employed with the agency.

SECURITY INCIDENT PROCEDURES

All HMIS Participating Agencies and their authorized users must abide to the terms of the HMIS agreements. Failure to fulfill these agreements may result in immediate termination of HMIS access until issues are resolved. All breaches related to security or privacy must be reported to the HMIS Lead immediately (within 24 hours) of discovery. The HMIS Participating Agencies assumes all liability due to data breaches or risk of incident within their organization.

All HMIS users are obligated to report suspected instances of noncompliance with these Standards that may leave HMIS vulnerable to intrusion or compromise client information. The HMIS Lead Agency/Administrator is responsible for reporting any security incidents involving the real or potential intrusion.

All HMIS users will report any incident in which unauthorized use or disclosure of client information has occurred. Security breaches that have the possibility to impact the HMIS must be reported to the HMIS Participating Agency Administrator who notified the HMIS Lead Agency/Administrator. Each HMIS Participating Agency will maintain and follow all procedures established by the HMIS Lead Agency, HMIS software, and Continuum of Care related to thresholds for security incident reporting.

The HMIS Lead Agency staff, in conjunction with the HMIS Administrator will review violations and recommend corrective and disciplinary actions. Each TPCH Partner Agency will maintain and follow procedures related to internal reporting of security incidents.

AUDIT AND ACCESS CONTROLS

The HMIS Lead Agency will maintain an accessible audit trail that allows the monitoring of user activity. The HMIS will also authenticate user activity via Internet Protocol (IP) address and prevent simultaneous user access.

All HMIS users are setup so that the HMIS uses the IP to validate the user. At no time and under no circumstance should an HMIS user share their user login and password or allow anyone to use their license. Each user is assigned a license.

PERSONNEL AUTHENTICATION & PASSWORD PROTOCOLS

All users are required to attend New User Training to obtain an HMIS license.

The below outlines password and user inactivity protocols for the each HMIS user:

1) All passwords must be unique,
2) All passwords must be rotated every 45 days,
3) All passwords must be in a prescribed format,
4) Upon the third unsuccessful login try, users will be locked out of the system and the HMIS administrator must reset.
5) All users with no login activity for at least 45 days will be automatically inactivated.

Locked out users will have to contact the HMIS administrator to have their account reactivated. All users with no login activity for at least 90 days will be automatically deactivated. The HMIS Administrator must be notified and will then have to reactivate. Users who reactivate after 6 months will be required to attend a New User Training for their license to be reactivated.

PUBLIC ACCESS PROTOCOLS

Program staff should be present to monitor workstations containing access to the HMIS. Additionally, when workstations are not in use and staff are not present, steps should be taken to ensure that the computers and data are secure and not usable by unauthorized individuals. After a short amount of time, workstations should automatically turn on a password protected screen saver when the workstation is temporarily not in use. Password protected screen savers are a standard feature with most operating systems and the amount of time can be regulated by the HMIS Participating Agency. If staff from an HMIS Participating Agency will be gone for an extended period of time, staff should log off the data entry system and shut down the computer. The HMIS will automatically log users out after 15 minutes of inactivity.

Malware and Virus Protection with Auto Update

HMIS Participating Agencies accessing the HMIS must protect the system by using commercially available malware, virus protection software, and must also maintain a secure firewall.

The HMIS Software Provider places firewalls on all data-hosting servers and regularly monitors all activity.

DISASTER PROTECTION AND RECOVERY

The HMIS Software Provider is contractually required to back up all HMIS data. Data back-up is conducted every 24 hours and is maintained using both power and alternative power systems at a different location from the primary HMIS server.

Encryption

SSL (Secure Sockets Layer) is standard security technology for establishing an encrypted link between a website and a browser. The HMIS Software Provider ensures that HMIS SSL certificates are maintained and the SSL encryption ONLY encrypts data going across the Internet to the end-user's web brower. The traffic that then flows between the server and the end-user's workstation is encrypted using the SSL certificate installed on that server.

At no time should client information be sent un-secured outside the HMIS software. Any email or other electronic correspondence regarding should be secured by the user and HMIS Participating Agency.

HMIS PARTICIPATING AGENCY AGREEMENT

Pima County Homeless Management Information System (HMIS)

This agreement is entered into by and between the Pima County, through the Community Services, Employment and Training Department ("CSET"), and ____________________________
____("AGENCY") located at ______
____
____.

The U.S. Department of Housing and Urban Development ("HUD") and the Tucson Pima Collaboration to End Homelessness ("TPCH"), the local Continuum of Care ("CoC"), have designated CSET the Homeless Management Information System ("HMIS") Grantee. As the HMIS Grantee, CSET is the HMIS Lead Agency responsible for implementing and operating the HMIS system and data collection requirements. The "HMIS System" is an internet-based management information software system.

This Agreement shall be effective on the date signed below and shall remain in effect until terminated in writing by either Party or until HUD and/or the CoC require execution of a new Agreement.

By signing below, the Parties agree to the following **Terms, Conditions and Responsibilities**:

A. **CSET**. CSET will perform the duties of the HMIS Lead Agency, which include, but are not limited to:

1. Approve use of HMIS System by AGENCY.
2. Procure, and retain sole ownership of, HMIS hardware and software.
3. Require the HMIS software developer to provide disaster recovery and data security controls.
4. Control the use and dissemination of all data entered into the HMIS System, pursuant to HUD regulations and the TPCH HMIS Protocol.

B. **AGENCY**. AGENCY provides services through various HUD-funded agreements that require it to enter data into the HMIS system. To use the HMIS System, AGENCY shall:

1. Ensure that Agency Administrator(s), or, if no Agency Administrator is available, an HMIS User, attends all mandatory HMIS Committee meetings and communicates HMIS business with other Agency HMIS Users.
2. Follow HMIS Procedures regarding timely entry of data into HMIS System.

3. Maintain a high level of data quality, ensuring that such quality is reviewed no less than monthly.

4. Immediately resolve data discrepancies and inconsistencies to ensure data integrity and accuracy for reports to HUD and the CoC.

5. Ensure that, if AGENCY uses the HMIS System to maintain data on non-HUD funded client services, such use has no impact on the data integrity and operation of the HMIS System.

6. Determine the specific individuals that will be allowed to enter data into the HMIS System, obtain authorization from CSET for each individual to use the HMIS System, and obtain a license for each specific individual. **AGENCY MAY NOT ALLOW AN INDIVIDUAL TO ACCESS THE HMIS SYSTEM PRIOR TO CSET AUTHORIZATION AND PROPER LICENSING.**

7. Ensure that each individual authorized to enter data into the HMIS System has a secure user ID and password. **UNDER NO CIRCUMSTANCES SHALL AGENCY ALLOW THE SHARING OF USER IDS AND PASSWORDS NOR THE USE OF AN USER ID AND PASSWORD BY ANY INDIVIDUAL NOT SPECIFICALLY AUTHORIZED BY CSET.**

8. Notify CSET immediately when an authorized HMIS User leaves the Agency's employment and ensure that no other individual has the ability to use that individual's HMIS System user ID and password.

9. Contact CSET regarding HMIS System software and technical assistance needs. Absent written approval from CSET, **AGENCY MAY NOT CONTACT THE HMIS SYSTEM SOFTWARE PROVIDER FOR ANY REASON, INCLUDING REQUESTING MODIFICATION OF THE SOFTWARE.**

10. Ensure that all authorized HMIS Users adhere to the HMIS Privacy Policies and Protocols and develop an internal HMIS Privacy Policy to prevent unauthorized, inappropriate, or illegal use of the data entered into the HMIS System.

11. Obtain a signed "Client Release of Information" form from each client and ensure that the executed releases are maintained in a secure and controlled location.

12. Designate at least one Agency Administrator to monitor AGENCY's use of the HMIS System and adherence to all privacy policies and CSET and CoC directives.

13. Comply with HUD HMIS Data and Technical Standards which is attached as **Exhibit A**, except when these Standards conflict with Arizona law. In such cases, Arizona law supersedes these Standards.

14. Ensure staff workstations are configured in a manner that prevents access to and viewing of the HMIS System data by anyone not specifically authorized and approved to see the data.

15. Not export client data from the HMIS System to any other organization, entity, government unit or person without first obtaining written permission from CSET.

16. Maintain secure Internet connectivity and computers for approved HMIS users.

C. **Indemnification**. AGENCY shall indemnify, defend, and hold harmless COUNTY, its officers, employees and agents from and against any and all suits, actions, legal administrative proceedings, claims or demands and costs attendant thereto, arising out of any act, omission, fault or negligence by the SUBGRANTEE, its agents, employees or anyone under its direction or control or on its behalf in connection with performance of this Grant Agreement.

D. **Termination**. CSET has the right to terminate this Agreement at any time it determines that AGENCY has failed to comply with its responsibilities under this Agreement.

AGENCY agrees to abide by the terms, conditions and responsibilities set forth in this Letter of Agreement. CSET agrees to perform the responsibilities set forth above. Further, CSET hereby authorizes AGENCY to use the HMIS System in the conduct of its activities pursuant to the terms and conditions set forth above. This Agreement supersedes and replaces any other agreement, oral or written, regarding the use of the HMIS System.

AGENCY (authorized signature):

____________________________________ __________________
Executive Director Date

CSET (approval):

____________________________________ __________________
Director Date

Pima County HMIS
Agency Administrator Agreement

____ "Agency"
Agency Name

Agency designates the following individual as HMIS Administrator: ______________________
The Agency HMIS Administrator is the primary contact for all communication regarding Pima County HMIS at this agency. Agency will ensure that the HMIS Administrator complies with all requirements set forth below. The Agency Administrator must acknowledge acceptance of the following responsibilities by initialing in the space provided:

_____ Coordinate Confidentiality Training, when available.

_____ Maintain executed "Client Release of Information" forms in a **secure** location.

_____ Request username and password authorizations from the Pima County HMIS Administrator for HMIS user at Agency.

_____ Monitor user adherence to workstation security and client information confidentiality policies.

_____ Ensure adherence to both the Agency's and Pima County's HMIS Protocols, policies and procedures.

_____ Provide technical support to Agency HMIS users, as needed.

_____ Regularly check accuracy of data entered into HMIS by Agency HMIS users, provide training and guidance.

_____ Monitor use of HMIS for data quality and timeliness.

_____ Regularly run data quality reports and work with Agency's HMIS users to implement corrective measures, as necessary.

_____ Immediately cancel Agency's HMIS user authorization upon separation of user from Agency.

_____ Notify Pima County HMIS Administrator of any changes in authorized users.

I understand and agree to comply with all statements initialed above.

____
Print Partner Agency Administrator Name

________________________________ ________________
Partner Agency Administrator Signature Date

________________________________ ________________
Partner Agency Executive Director Signature Date

________________________________ ________________
Pima County HMIS Lead Agency Signature Date

Pima County HMIS User Agreement

____(“Agency” or “Employer”)
Agency Name

Agency designates the following individual as an HMIS User: _________________________________
HMIS User Name

The above-named HMIS User is an individual who works directly with clients to obtain information from and enter data regarding clients into the Pima County Homeless Management Information System (“HMIS System”) or who accesses the data from the HMIS System in the course of performing his or her duties for the Agency. Agency will ensure that this HMIS User complies with all requirements set forth below.

My initials in the spaces provided below, and my signature, are proof that I understand, accept and agree to comply with the following HMIS System User requirements:

1. **HMIS DATA CONFIDENTIALITY**:

_____ **The information entered into the HMIS system is sensitive and confidential, and is not to be shared, disseminated, discussed or otherwise disclosed**, except as specifically instructed by my Employer or as directed in writing by the client.

_____ **Unauthorized, inappropriate, or illegal use of the data entered into the HMIS System may subject me to discipline and/or criminal penalties**.

_____ The data that I am able to access in the HMIS System is not to be viewed by or shared with any other HMIS User either in my Agency or in another Agency unless specifically authorized by my Employer and the Pima County HMIS System Manager or as specified in a written request of the client.

_____ I may only view, obtain, disclose or use data in the HMIS System as necessary to perform my job duties and responsibilities associated with providing services to my Agency’s clients.

_____ Information in the HMIS System about an individual client may only be shared with that client.

_____ I must immediately report any suspected or actual security breach to the HMIS Agency Administrator or the Pima County System Administrator.

2. **HMIS USER ID AND PASSWORD CONFIDENTIALITY**:

_____ My HMIS user ID and password **may not be accessible to, shared with or given to any other person**.

_____ My HMIS user ID and password will be kept in a secure location that prevents anyone else from seeing and learning what they are.

_____ If I leave employment at the Agency, I will not give my HMIS user ID and password to anyone else in the Agency or to the new person assuming my job.

3. **COMPUTER SECURITY**:

_____ **I will never leave my computer unattended when I am logged into the HMIS System**.

_____ If I leave my computer and work area, I will log out of the HMIS System and close the internet browser.

4. **DATA ENTRY**:

_____ **The computer's automatic data saving must be set to occur every four (4) minutes**.

_____ HMIS data must be entered according to AGENCY policies and Pima County HMIS data standards.

_____ I will be careful when entering data into the HMIS System to be accurate.

_____ The following will NOT be entered into the HMIS System, unless a direct quote of a client AND essential to assessment, services or treatment:

> _____ **Discriminatory comments** by or about any person regarding race, color, religion, national origin, ancestry, discrimination, age, sex, or sexual orientation.
>
> _____ **Offensive language and/or profanity**.

5. **FAILURE TO COMPLY**:

_____ I may be subject to personnel action, including, but not limited to termination from employment or volunteer status with the Agency if I fail to comply with the provisions of this User Agreement.

Printed HMIS User Name	HMIS User Job Title
HMIS User Signature	Date
Agency Executive Signature	Date
HMIS Agency Administrator Signature	Date
Pima County HMIS Administrator Signature	Date