1 Haven for Hope Way, San Antonio, Texas 78207

Homeless Management Information System (HMIS) Policies & Procedures

Approved: December 2021

San Antonio / Bexar County Continuum of Care

Developed by: HMIS Lead Agency and SARAH

Approved by: CoC Board of Directors

TABLE OF CONTENTS

Date	Version	Description
12/29/2011	1.0	HMIS Policies & Procedures
08/11/2016	2.0	CoC Board of Directors approval date
02/2020	3.0	CoC Board of Directors approval date
06/2020	3.1	CoC Board of Directors approval date
09/2021	4.0	CoC Board of Directors approval date

1. OVERVIEW

1.1 PURPOSE OF HMIS

The McKinney-Vento Homeless Assistance Act, as amended by the Homeless Emergency Assistance and Rapid Transition to Housing Act of 2009 (HEARTH), requires that the U.S. Department of Housing and Urban Development (HUD) ensure operation of community-wide Homeless Management Information System (HMIS) with consistent participation by recipients and sub-recipients of applicable federal grants. The HMIS has many uses, including:

- Collecting unduplicated counts of individuals and families experiencing homelessness;
- Analyzing patterns of use of assistance provided in a community; and,
- Providing information to project sponsors and applicants for needs analyses and funding allocations.

Additionally, HMIS is essential to coordinate services, evaluate performance, ensure accountability in the use of public funds, and inform public policy. Ultimately, the HMIS serves as the foundation for all planning to prevent, reduce, and eliminate homelessness.

The HMIS Lead Agency for the San Antonio/Bexar County Continuum of Care (CoC) is Haven for Hope (H4H). In addition to administering the local HMIS, the HMIS Lead must develop written policies and procedures for all HMIS participating agencies in the CoC, execute participation agreements with each of these agencies and their system users, and monitor and enforce compliance by all participating agencies with the requirements set forth in the participation agreement. The HMIS Lead is responsible for maintaining the HMIS Policies and Procedures manual and all related documents, training system users, and providing technical assistance.

The HMIS software vendor for San Antonio/Bexar County CoC is CaseWorthy, Inc. Accordingly, the HMIS application may be referred to as “CaseWorthy” in operational manuals.

1.2 KEY TERMS

1. Continuum of Care: a community-based collaborative that oversees homeless system planning and coordination, including the HMIS implementation.

2. HMIS Lead Agency: the organization that administers and operates the HMIS.

3. Participating Agency: any agency that contributes data or uses the HMIS.

4. Exempt Agency: any agency that is explicitly exempt from entering data into the HMIS by federal regulations. This includes victim services providers.

5. Client: a person who receives services at an HMIS participating agency.

6. Personally Identifiable Information (PII): Defined in OMB M-07-16 as "...information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.".

1.3 DATA OWNERSHIP

1.3.1 DATA OWNERSHIP POLICIES

1. The CoC Lead Agency and the Contributory HMIS Organization (CHO) maintain joint ownership of the data entered into HMIS by the CHO.

- A CHO can only request data entered into HMIS by their organization or into a project owned by their organization.
- A CHO can elect to no longer enter data into HMIS and may receive a copy of previously entered data, however, the data cannot be removed from the system.

2. Universal Data Elements are universally owned and can be requested by anyone who has entered data on the client's profile.

3. For projects with joint ownership, a primary and secondary owner must be established

- The primary owner maintains ownership of all data entered in the project.
- The secondary owner may request data entered by their organization.
- SARAH maintains primary ownership of Homelink data, but CHO's may request data that their organization entered.

Procedures:

1. In the event that the HMIS system ceases to exist, participating agencies will be notified and provided reasonable time to access and save data on persons served by the participating agency. Thereafter, the information collected in the HMIS will be purged or appropriately stored.

2. In the event that H4H ceases to exist or is no longer the administrator of the HMIS, the CoC Board will select a new HMIS Lead and transfer the custodianship of the data within HMIS to another organization for continuing administration. In such event, participating agencies will be informed in a timely manner.

1.3.2 REQUESTING DATA

1. When requesting data, the organization must identify all data elements being requested.

- Organizations may request Universal Data Elements, Program Specific Data Elements, and custom data elements.

2. If data that is not linked to a project enrollment is requested (e.g. Case Notes), the HMIS Team will provide data linked to the Organization ID of the requestor.

3. Data requests must follow data ownership policies. Any data requested beyond the scope of ownership follows the CoC Data Use Agreement and request process. This information may be accessed at the following link: https://sarahomeless.org/reports-and-data/#request-data

1.4 VOLUNTARY PARTICIPATION

The CoC Board strongly encourages agencies that serve persons who are homeless or at risk of homelessness and are not required to participate in HMIS to do so voluntarily.

Having more homeless service providers in the HMIS creates the potential for:

- More effective coordination of client services through case management and referral information sharing;

- More accurate tracking of client returns to the homelessness prevention and assistance system;
- More accurate counts of homeless persons and system resources, which could be used to understand the gaps in the service system;
- Better information about community-wide needs, which can help guide advocacy efforts, policymaking, and funding allocations; and
- Better information about system outcomes, which can be used to guide service targeting and performance improvement efforts.

1.5 HMIS DOCUMENTATION AMENDMENT PROCESS

1.5.1 POLICIES

The HMIS Lead and HMIS Advisory Committee will guide the amendment of HMIS Policies and Procedures and other related documentation.

The HMIS Advisory Committee will approve the HMIS Policies and Procedures and Data Quality Plan.

1.5.2 PROCEDURES

1. Proposed changes may originate from any participant in HMIS, including clients.

2. When proposed changes originate within a participating agency, they must be reviewed by the Executive Director/Program Director (or equivalent) and then submitted to the HMIS Manager.

3. The HMIS Manager will maintain a list of proposed changes.

4. The list of proposed changes will be discussed by the HMIS Advisory Committee at the next regularly scheduled meeting. At this meeting, the committee will determine if these changes require additional research and if so, they will create a plan for completing the necessary research.

5. If changes do not require additional research or once this research is complete, then the committee will vote on whether or not to propose these changes to the HMIS Lead.

6. Changes approved by the HMIS Advisory Committee will be made by the HMIS Manager and sent to all HMIS participating agencies.

7. The Executive Director/Program Director (or equivalent) from each of the agencies shall acknowledge receipt and acceptance of the revised HMIS Policies and Procedures (or other documents) within 10 working days of delivery of the amended document by notification in writing or email to the HMIS Manager. The agency's Executive Director/Program Director (or equivalent) shall also ensure the circulation and compliance of the revised policies and procedures within their agency.

8. Trainings on changes to HMIS documentation will be scheduled as needed.

2. STAKEHOLDER RESPONSIBILITIES

2.1 COC BOARD

1. Select and designate an HMIS Software for the CoC.

2. Select and designate an HMIS Lead for the CoC, among eligible applicants.

3. Work with the HMIS Lead to ensure consistent agency participation across the CoC.

4. Evaluate performance of the HMIS Software and HMIS Lead.

2.2 HMIS ADVISORY COMMITTEE

1. Review and approve HMIS Policies and Procedures.

2. Review and approve the Data Quality Plan.

3. Gather and incorporate user feedback into the HMIS Policies and Procedures.

4. Provide feedback on HMIS documentation.

5. Participate in efforts to promote HMIS operations, research, and analysis.

2.3 HMIS LEAD AGENCY

1. H4H is responsible for the administration of the HMIS project under the auspices of the CoC Board, which authorizes H4H to hold the HUD HMIS grant.

2. H4H shall maintain an HMIS Department with, at minimum, 5 full-time employees, or their equivalent, dedicated solely to those HMIS responsibilities set forth in this section. These responsibilities are grouped by function, though actual H4H job titles and descriptions may differ.

3. H4H shall establish an HMIS Ticketing System, enabling participating agencies and system users to receive professional technical assistance. Additional resources and contact information for the help desk can be found here: https://www.havenforhope.org/hmis-resources/.

2.3.1 HMIS MANAGER

1. Oversee the collection, analysis and presentation of HMIS data for reporting to federal, state, and local governments, and private entities.

2. Oversee HUD HMIS grant application and reporting process.

3. Oversee the overall administration of the HMIS software.

4. Oversee HMIS Department activities and staff as described in this section.

5. Oversee HMIS help desk and designate staff responsibility to manage, coordinate and support its operation.

6. Lead performance and staff evaluation activities.

7. Engage with new and current participating agencies to identify business needs; identifying opportunities for customization within the HMIS application.

8. Work with H4H's Senior Director of Transformational Services to develop and implement strategic plan for HMIS, evaluate priorities, and promote a continuous improvement environment to advance training and technical assistance.

9. Perform other duties as assigned.

2.3.2 HMIS LEAD SYSTEM ADMINISTRATOR

1. Leads team in maintaining system performance.

2. Maintains security, maintenance, backups, and capacity of the HMIS database.

3. Leads team in identifying data quality problems, developing remedies, suggesting and implementing corrective and/or preventative actions.

4. Leads team in system troubleshooting and continuous improvement efforts.

5. Establishes team standards and practices for monitoring timely and accurate completion of critical data elements and processes.

6. Provides technical guidance in identifying and defining data elements stored in the system.

7. Reviews data queries and reports for accuracy.

8. Leads team in implementing required HUD Federal Reports and Data Standards requirements.

9. Assists user organizations in requirements gathering, process documentation, and other business analysis.

10. Establishes and maintains documentation, change management, and testing, and development procedures for customization and enhancements.

11. Coordinates activities related to software updates and upgrades, including communication with HMIS manager and other organization staff, software testing, and implementation scheduling.

2.3.3 HMIS SECURITY AND COMPLIANCE COORDINATOR

1. Complete site visits at participating agencies to monitor compliance with HMIS Policies and Procedures.

2. Assist in developing the HMIS Security Plan.

3. Document reports of suspected violations of client privacy or data security policies, participating agency responses, and HMIS Lead responses.

4. Coordinate with HMIS Manager regarding HMIS Lead responses to suspected violations of client privacy and data security policies.

5. Coordinate with participating agencies regarding agencies policy of disposal of electronic devices where clients' Protected Health Information (PHI) was stored.

6. Serve as point of contact on HMIS Data Standards compliance, staying abreast of any changes.

7. Maintain the HMIS Policies and Procedures document, making updates and revisions as needed.

8. Ensure compliance with HUD HMIS Data and Technical Standards and H4H's HMIS Policies and Procedures.

2.3.4 HMIS TRAINING COORDINATOR

1. Conduct Training for all HMIS Users, which includes but is not limited to HMIS Security Awareness Training, HMIS Fundamentals Training, Elements of Focus Training, Program Specific Training, Report Training, Chronic Homeless Definition Training, System Performance Measures Training, Point in Time Training.

2. Responsible for providing and creating training materials, including training guides, tutorial videos, and other resources as requested.

3. Provide technical guidance on HMIS implementation to participating agencies.

4. Perform other duties as assigned.

5. Conduct annual security trainings for system users.

2.3.5 HMIS SYSTEM ADMINISTRATOR

1. Oversee HMIS system performance; create database backups, triggers, and indexes.

2. Work closely with HUD and HMIS software vendor to ensure compliance.

3. Maintain contact with HMIS software vendor to ensure optimal performance.

4. Ensure the HMIS database is secure and not over capacity.

5. Identify problematic areas and conduct research to determine the best course of action to correct the data.

6. Analyze and solve issues with current and planned systems as they relate to the information and management of client data.

7. Analyze reports of data duplicates or other errors to provide ongoing appropriate interdepartmental communication and monthly or daily data reports.

8. Perform other duties as assigned.

2.3.6 HMIS DATA QUALITY ANALYST

1. Work with participating agencies to maintain accurate Housing Inventory Count within HMIS.

2. Work with HMIS Advisory Committee to devise and monitor quality benchmarks.

3. Assist in defining specifications for updates to data elements in the HMIS.

4. Assist participating agencies with performance evaluation activities.

5. Complete data analysis projects, as assigned by the HMIS Manager.

6. Fulfill external data requests as approved the HMIS Manager.

7. Provide support to system users in their use of HMIS data.

8. Perform other duties as assigned.

2.3.7 HMIS APPLICATION SUPPORT SPECIALIST

1. Manage, assign, and follow-up with tickets, using the HMIS ticketing system.

2. Provide technical assistance to system users.

3. Complete HMIS software customizations.

4. Activate and disable user accounts.

5. Assist with data monitoring within the HMIS.

6. Perform other duties as assigned.

2.4 PARTICIPATING AGENCY

2.4.1 AGENCY EXECUTIVE DIRECTOR/PROGRAM DIRECTOR

1. Sign the Contributory HMIS Organization (CHO) Agreement and submit it to the HMIS Security and Compliance Coordinator.

2. Ensure agency compliance with the terms and conditions of the CHO Agreement and HMIS Policies and Procedures.

3. Ensure personnel with access to the HMIS comply with the terms and conditions of the Security Awareness Agreement.

4. Designate one employee as the agency's HMIS Representative to serve as the primary point-of-contact on HMIS operations at the agency.

5. Designate one employee as the agency's HMIS Security Officer and notify the HMIS Security and Compliance Coordinator of this assignment.

6. Support the HMIS Leads effort to resolve HMIS data quality and compliance issues.

2.4.2 AGENCY HMIS REPRESENTATIVE

1. Ensure compliance with HMIS data collection, data entry and reporting requirements as outlined the HMIS Policies and Procedures.

2. Serve as primary point-of-contact for communication between the agency and HMIS Lead on HMIS operations.

3. Provide support on resolution of any data quality and reporting issues.

4. Identify agency personnel to access the system and receive HMIS training.

5. Sign Training Request Forms to authorize access.

6. Notify the HMIS help desk within 24 hours of relevant personnel changes to ensure system user accounts are deactivated.

2.4.3 AGENCY HMIS SECURITY OFFICER

1. Ensure compliance with the privacy and security standards as outlined in the HMIS Policies and Procedures.

2. Send a copy of the agency-specific data security policies and procedures to HMIS Security and Compliance Coordinator.

3. Send updated agency-specific data security policies and procedures to HMIS Security Officer within 30 days of any changes.

4. Ensure compliance with the agency-specific data security policies and procedures.

5. Document and investigate suspected violations of client privacy or data security policies.

6. Notify HMIS Security and Compliance Coordinator within 24 hours of receiving reports of suspected violations of client privacy and data security policies.

7. Notify HMIS Security and Compliance Coordinator of the agency's response to suspected violations of client privacy and data security policies.

2.4.4 SYSTEM END USER

1. Sign the Security Awareness Agreement electronically in HMIS.

2. Responsible for maintaining the electronic Security Awareness Agreement in HMIS.

3. Complete HMIS training and meet training objectives.

4. Comply with all HMIS agreements, policies and procedures.

5. Report suspected violations of client privacy and data security policies to the agency HMIS Security Officer.

6. Provide feedback to the HMIS Lead.

2.5 EXEMPT AGENCY

1. Utilize a comparable database to the HMIS.

2. Develop database policies and procedures that comply with federal HMIS regulations.

3. Submit policies and procedures to HMIS Security and Compliance Coordinator.

4. Ensure compliance with agency-level policies and procedures.

3. OPERATIONAL POLICIES AND PROCEDURES

3.1 HARDWARE, SOFTWARE, AND NETWORK REQUIREMENTS

Policy: The participating agency is responsible for meeting the minimum hardware, software, and network requirements to access the HMIS, and for providing the necessary maintenance for continued participation.

CaseWorthy is a web-based application that can be accessed from any desktop computer (PC or Mac). CaseWorthy does not work on mobile devices like smartphones, however does work on tablets and iPads. In order to access the HMIS, a computer must have one of the following browsers installed:

- Google Chrome 50.0 or above (Recommended)
- Firefox 40.0 or above
- Microsoft Edge

The device must also have a functioning internet connection.

3.2 SYSTEM ACCESS

3.2.1 POLICIES

•The participating agency is responsible for identifying personnel for system training and access.

•System users shall be assigned “roles” based on programmatic needs and considerations.

•The participating agency will notify H4H of any need to change “roles”.

•The participating agency will notify H4H of the need to deactivate system users within 24 hours of termination of their service with the agency. Advance notification is preferred, especially in the case of agency-initiated terminations.

3.2.2 PROCEDURES TO DESIGNATE A NEW SYSTEM USER

1. The authorized contact will submit a Training Request Form to the HMIS ticketing system, specifying the user’s first and last name, organization issued email address, role/title, and a description of HMIS-related job functions.

2. The authorized contact must ensure the user views the HMIS Security Awareness Training video and HMIS Fundamentals videos in their entirety before the user completes the Security Awareness Quiz and Fundamentals Quiz. Once the user receives a score of 80% or above on

each quiz, they will be scheduled for HMIS Elements of Focus Training (if required for their position) and granted HMIS access.

3. The HMIS Training Coordinator will schedule the user for HMIS Elements of Focus Training (if required for their position), then provide the user the HMIS Login Information email which contains credentials and instructions for the user to login to HMIS, change the password, and complete the Security Awareness Agreement.

4. If HMIS Elements of Focus Training is required, the HMIS Training Coordinator must receive training session confirmation by 3:00 p.m. the day prior to the scheduled session.

5. If HMIS Report Training is required, the HMIS Training Coordinator must receive training session confirmation by 10:00 a.m. the day prior to the scheduled session.

6. Once the user completes the required items in step 3, they will be granted HMIS access.

3.2.3 PROCEDURES TO CHANGE USER ROLE

1. The authorized contact will submit a Training Request Form to the HMIS ticketing system, specifying the user's first and last name, organization issued email address, role/title, and a description of HMIS-related job functions.

2. The HMIS Training Coordinator will either provide the required Fundamentals Training and/or schedule the user for an Elements of Focus Training. The user must complete the required training(s) prior to being assigned a new role.

3.2.4 PROCEDURES TO CHANGE USER AGENCY

1. The authorized contact will submit a Training Request Form to the HMIS ticketing system, specifying the user's first and last name, organization issued email address, role/title, and a description of HMIS-related job functions.

2. The HMIS Training Coordinator will provide the HMIS Security Awareness Training and either provide the required Fundamentals Training and/or schedule the user for an Elements of Focus Training. The user must complete the required training(s) prior to gaining HMIS access with the new agency.

3. If HMIS Elements of Focus Training is required, the HMIS Training Coordinator must receive training session confirmation by 3:00 p.m. the day prior to the scheduled session.

4. If HMIS Report Training is required, the HMIS Training Coordinator must receive training session confirmation by 10:00 a.m. the day prior to the scheduled session.

5. Once the user completes the required items in step 3, they will be granted HMIS access.

3.2.5 PROCEDURES TO DEACTIVATE A SYSTEM USER

1. The authorized contact will submit a user deactivation request to the HMIS ticketing system.

2. The HMIS help desk will deactivate the system user.

3.3 USER LICENSE ALLOCATION POLICIES

- Each Contributory HMIS Organization (CHO) is allocated a specified number of User Licenses based on category.

Category	A	B	C	D
Number of Licenses	50	20	5	2

- All current CHOs will be grandfathered in at current user count as of June 2021. However, requests for additional licenses are subject to this policy.
- If a CHO falls into multiple categories, the determination will be based on the category with the highest number of licenses.
- If a CHO requires additional licenses, a User License Increase Application may be submitted for consideration by the HMIS Advisory Committee.
- The application must be submitted by the Agency HMIS Security Officer.
- Prior to submitting the application, the Security Officer must review the list of active HMIS Users to determine if existing licenses may be reallocated to new staff members.
- The HMIS Manager will present the application to the Committee at the next meeting and inform the HMIS Security Officer of whether their application was approved.

- If a user's account is deactivated due to inactivity three times, the HMIS Security Officer must request approval from the HMIS Advisory Committee for the account to be restored.

3.4 DATA COLLECTION POLICIES

•The participating agency is responsible for understanding its HMIS compliance requirements as may be defined by various federal grant programs and funders, and fulfilling any contractual obligations, including but not limited to compliance reports.

•The participating agency is responsible for communicating these requirements to the HMIS Lead to ensure the system is properly configured to collect required data.

•The participating agency is required to collect and enter information into the HMIS as defined in the federal HMIS Data Standards Manual, specifically the Universal Data Elements (UDEs) and the Program Specific Data Elements (PDEs): https://www.hudexchange.info/resources/documents/HMIS-Data-Standards-Manual.pdf

•The participating agency will be required to collect Local Data Elements (LDEs) as defined as defined in the HMIS Data Quality Plan. Organizations and projects will be categorized into an A, B, C, or D category, which will define the required data needed to be entered into HMIS.

•The HMIS Lead must post information about LDEs and their applicability to participating agencies on H4H's HMIS support website.

•The HMIS Lead must provide training and technical assistance on Universal Data Elements (UDE)/ Project Descriptor Data Elements (PDDE).

3.5 DATA TRANSFER

3.5.1 POLICIES

•The participating agency is permitted to export data from HMIS to another system, once the agency has received approval from the HMIS Lead and CoC Lead to do so.

•The participating agency is responsible for adhering to federal, state and local privacy laws within their databases, if it transfers any client data outside of HMIS.

3.5.2 PROCEDURES

•The participating agency can request training from the HMIS Lead regarding data transfers by submitting a request to the HMIS help desk.

•The HMIS help desk will coordinate this training with the agencies.

3.6 TRAINING

3.6.1 POLICIES

•All new users are required to complete HMIS system training and security awareness training before being allowed access to the system.

•All active users are required to complete annual training on security awareness.

•All active users are required to participate in training on any updates to the system, policies or procedures, as needed.

•All users are required to sign the Security Awareness Agreement, acknowledging receipt of a copy of the privacy notice (see Section 5) and pledging to comply with the privacy notice and additional terms and conditions for HMIS access.

3.6.2 PROCEDURES

1. HMIS training increases user's understanding, knowledge, and skills to effectively use the HMIS database. HMIS training increases user's understanding, knowledge, and skills to effectively use the HMIS database.

2. All training must be requested through our Training Request using the following link: https://docs.google.com/forms/d/e/1FAIpQLSfNXXjIxJmFSckPonnPo0LRp1JmbXXLPjTAogWddiw-abawKQ/viewform

3. Training is offered in a combination of online and live formats. Training may be requested for entire departments or individual one-on-one sessions.

4. Optional and required trainings will be announced via email.

3.7 TECHNICAL ASSISTANCE

3.7.1 POLICIES

•The participating agency may request HMIS technical assistance from the HMIS Lead.

•Technical assistance is limited to the implementation and operation of HMIS for those authorized uses as defined in these HMIS Policies and Procedures.

3.7.2 PROCEDURE

•Requests for technical assistance can be submitted, through the online support ticketing system: HMIS.Support@havenforhope.org.

4. SECURITY POLICIES

4.1 PURPOSE

•These security policies are directed to ensure the confidentiality, integrity, and availability of all HMIS information; protect against any reasonably anticipated threats or hazards to security; and ensure compliance by end users.

•The Contributory HMIS Organization (CHO) Security Officer/Participating Agency Security Officer is responsible for preventing degradation of the HMIS resulting from viruses, intrusion, or other factors within the agency's control.

•The participating agency security officer is responsible for preventing inadvertent release of confidential client-specific information through physical, electronic or visual access to the workstation.

•Each participating agency security officer 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.

•To promote the security of HMIS and the confidentiality of the data contained therein, access to HMIS will be available via a secure network.

•End Users shall commit to abide by the governing principles of HMIS and adhere to the terms and conditions of the HMIS Security Awareness 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 Contributing 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.

4.2 USER SECURITY REQUIREMENTS FOR HMIS CATEGORIES

4.2.1 CATEGORY A AND B AGENCIES

•Annual security presentation.

•Adhere to HUD 2004 data security standards.

•Designate a Security Officer for monitoring compliance. This must be updated at least annually or within 15 days of staff transition.

•Inform HMIS of deactivating accounts within 24 hours an employee leaves the agency.

4.2.2 CATEGORY C AND D AGENCIES

•Annual security presentation.

•Adhere to HUD 2004 data security standards.

•Designate a Security Officer for monitoring compliance. This must be updated at least annually or within 15 days of staff transition.

•Inform HMIS of deactivating accounts within 24 hours an employee leaves the agency.

•Must consistently login to HMIS. A user that has their HMIS Account deactivated more than 3 times or has not logged into HMIS within 30 days will have their HMIS access removed.

•Viewing only agencies will be limited to two HMIS Users.

4.3 SYSTEM APPLICABILITY

•The participating agency and HMIS Lead, including any authorized agents, must follow the security policies established in this section.

4.4 DISASTER RECOVERY PLAN

•Disaster Recovery for the San Antonio/Bexar County HMIS will be conducted by the HMIS Lead Agency, in collaboration with the HMIS vendor CaseWorthy and Haven for Hope IT department Topbox, as well as Azure.

•The Lead Security Officer should maintain ready access to the following information:

•Contact information – Phone number and email address of CaseWorthy and TopBox contacts responsible for recovering the agency's data after a disaster.

•Agency responsibilities – A thorough understanding of the agency's role in facilitating recovery from a disaster.

•All HMIS System Administrators should be aware of and trained to complete any tasks or procedures for which they are responsible in the event of a disaster.

•The HMIS System Administrator/TopBox must have a plan for restoring local computing capabilities and internet connectivity for the HMIS System Administrator's facilities. This plan should include the following provisions.

- Account information – Account numbers and contact information for support contracts.
- 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 participating agencies.
- Network and system configuration information – Documentation of the configuration settings required to restore local user accounts and internet access.

4.5 SECURITY MANAGEMENT AND COMPLIANCE, AND ANNUAL REVIEW

•The HMIS Lead is responsible for managing the selection, development, implementation, and maintenance of security measures to protect HMIS information.

•The HMIS Lead must retain copies of all contracts and agreements executed as part of the administration and management of the HMIS or otherwise required.

•The HMIS Lead must complete an annual security review to ensure the implementation of the security requirements for itself and the participating agency, using a checklist to ensure compliance with each requirement defined in this section.

4.6 SECURITY OFFICERS

•The participating agency and HMIS Lead must each designate an agency representative to serve as HMIS Security Officer to be responsible for compliance with applicable security policies (see Stakeholder Responsibilities).

4.7 HMIS LEAD SECURITY OFFICER

•May be an HMIS System Administrator or another employee, volunteer or contractor designated by the HMIS Lead Agency who has completed HMIS Privacy and Security training and is adequately skilled to assess HMIS security compliance, Assesses security measures in place prior to establishing access to HMIS for a new participating agency, Reviews and maintains file of participating agency annual compliance certification checklists, conducts annual security audit of all participating agencies. At this time, this role will be assumed by the HMIS Security and Compliance Coordinator.

4.8 CONTRIBUTORY SECURITY OFFICER/PARTICIPATING AGENCIES SECURITY OFFICER

•May be the agency's Technical Administrator or another employee within the agency, volunteer or contractor who has completed HMIS Privacy and Security training and is adequately skilled to assess HMIS security compliance,

•Conducts a security audit for any workstation that will be used for HMIS data collection or entry

•Continually ensures each workstation within the participating agency used for HMIS data collection or entry is adequately protected by a firewall and antivirus software (per Technical Safeguards – Workstation Security),

•Completes the Compliance Certification Checklist and forwards the Checklist to the HMIS Security & Compliance Coordinator.

4.9 SECURITY AUDIT

New HMIS Participating Agency Site Security Assessment

•Prior to establishing access to HMIS for a new agency, the HMIS Security & Compliance Coordinator will assess the security measures in place at the new participating agency to protect client data (see Technical Safeguards – Workstation Security). The HMIS Security & Compliance Coordinator will meet with the Agency Executive Director (or executive-level designee), agency's HMIS Technical Administrator and/or agency Security Officer to review the agency's information security protocols. This security review shall in no way reduce the agency's responsibility for information security, which is the full and complete responsibility of the Agency, its Executive Director, and its Technical Administrator/Security Officer.

4.10 PARTICIPATING AGENCY SELF-AUDIT

4.10.1 PARTICIPATING AGENCY SELF-AUDIT POLICIES

•The Participating Agency Security Officer will use the Compliance Certification Checklist to conduct security audits on their Agency workstations.

•The Participating Agency Security Officer can request HMIS logins to compare to employee time sheets during periods of remote access.

•If areas are identified that require action due to noncompliance with these standards or any element of the San Antonio/Bexar County HMIS Policies and Procedures, the participating agency security officer will note these on the Compliance Certification Checklist, and the Agency Security Officer and/or HMIS Technical Administrator will work to resolve the action item(s).

•Any Compliance Certification Checklist that includes 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

participating agency Executive Director or other empowered officer prior to being forwarded to the HMIS Lead Security and Compliance Coordinator.

•The Participating Agency Security Officer must turn in a copy of the Compliance Certification Checklist to the HMIS Security & Compliance Coordinator on a quarterly basis.

4.10.2 QUARTERLY SELF-AUDIT WORKFLOW

1. HMIS Quarterly Self-Audit Sent

HMIS Security and Compliance Coordinator sends the quarterly self-audit information to the Agency Security Officer by the 3rd business day of the quarter. The Agency Security Officer will complete the Compliance Checklists and return them no later than last business day of the month.

2. HMIS Reminder

If no response by the 15th of the month, an email reminder will be sent to the Agency Security Officer on the following business day.

3. Final HMIS Reminder

If the checklists have not been returned by the deadline, the HMIS Security and Compliance Coordinator will send a follow-up email informing the Agency Security Officer of the past due self-audit. The agency will have 3 additional days to return the completed checklists.

4. SARAH Involvement

If still no response after 3 days, SARAH's Data Coordinator is notified at next HMIS Operations Meeting, which occurs every Wednesday. SARAH's Planning Manager will reach out to the project point of contact. The HMIS team is notified when this outreach takes place. If still no response, the CoC Contract will be evaluated, if one exists.

5. HMIS Advisory

As Category B, C, and D do not have CoC contracts, the decision at this point is whether the project should still be allowed HMIS access. This decision will be made by the HMIS Advisory Committee.

4.10.3 QUARTERLY SELF-AUDIT PROCEDURES

Agencies review 5% of users or 10 total, whichever is less.

Percentage of client data audit is based on performance on last audit:

0-30% Accuracy Error Rate = 3% of client records audited.

31-60% Accuracy Error Rate = 5% of client records audited.

61-100% Accuracy Error Rate = 10% of client records audited.

4.11 SECURITY AUDITS

1. The HMIS Security & Compliance Coordinator will schedule the security audit in advance with the participating agency Security Officer.

2. The HMIS Security & Compliance Coordinator will use the Compliance Certification Checklist to conduct security audits.

3. The HMIS Security & Compliance Coordinator must randomly audit workstations for each HMIS participating agency. In the event that an agency has more than 1 program site, each 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 San Antonio/Bexar County HMIS Policies and Procedures, the HMIS Security & Compliance Officer will note these on the Compliance Certification Checklist, and the participating agency security officer and/or technical administrator will work to resolve the action item(s).

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 participating agency Executive Director or other empowered officer and forwarded to the HMIS Security & Compliance Coordinator.

4.12 SECURITY AWARENESS TRAINING

•The HMIS Lead must ensure that all system users receive security training before being given access to the system and at least annually thereafter. The HMIS Lead will maintain attendance records for all training events to assure compliance.

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.

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 participating agency's 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, such as privacy screens.

Technical Safeguards

Workstation Security

1. The participating agency security officer will confirm that any workstation accessing HMIS shall have antivirus software with current virus definitions and frequent full system scans. This may be verified through the agency's technical department.

2. The participating agency security officer will confirm that any workstation accessing HMIS has and uses a hardware or software firewall. This may be verified through the agency's technical department.

3. The participating agency must ensure that devices used to access the HMIS are password protected with automatic system lock out after user inactivity.

4. The participating agency must ensure that the internet connections used to access HMIS from their facilities are set up using network security protocols to prevent unauthorized access to the network and to HMIS data saved locally.

5. Due to the confidential nature of data stored within HMIS, the system must be accessed from a sufficiently private physical location so as to ensure that persons who are not authorized users of the HMIS are not able to view client level data.

Establishing HMIS User IDs and Access Levels

1. The participating agency Technical Administrator is responsible for ensuring that all agency End Users have completed mandatory trainings, including HMIS Privacy, Security training and End User Responsibilities and Workflow training, prior to being provided with a User ID to access HMIS.

2. The participating agency Technical Administrator will ensure all users are up to date with HMIS Security Awareness Agreements.

3. All End Users will be issued a unique User ID and temporary password to initially access the system, then they will need to create their own 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.

4. The HMIS Lead will always attempt to assign the most restrictive access that allows the End User to efficiently and effectively perform his/her assigned duties.

5. The HMIS Lead will create the new User ID and notify the User ID owner of the temporary password during HMIS New User Training.

6. When the participating agency Technical Administrator determines that it is necessary to change a user's access level, the contributory Agency Technical Administrator will notify the HMIS Team via ticketing system, so the HMIS Team may update user account as necessary.

Passwords

1. Temporary passwords must be changed on first use. User-specified passwords must be a minimum of 6 characters long and must contain at least one lowercase letter, at least one uppercase letter, at least one number, and at least one special character [!@#$%&*].

2. HMIS End users will be prompted by the software to change their password every 90 days.

3. HMIS End Users must immediately notify their participating agency technical administrator if they have reason to believe that someone else has gained access to their password as well as the HMIS Team Lead via the ticketing system.

4. Three consecutive unsuccessful attempts to login will disable the User ID for 30 minutes. For HMIS End Users, passwords should be reset by the End User by using the "Forgot Password" feature or the HMIS Lead Team via ticketing system.

5. HMIS End User must not allow their internet browser to save their HMIS password.

6. System users must not store their password in locations that are easily accessible to others (i.e. under the computer keyboard or posted near their workstation).

Rescinding User Access

1. End User access should be terminated by the HMIS Team Lead within 24 hours if an End User no longer requires access to perform his or her assigned duties due to a change of job duties or termination of employment. The contributory agency's security officer must notify the HMIS Team Lead immediately via ticketing system.

2. The HMIS System Administrator reserves the right to terminate End User licenses that are inactive for 90 days or more.

3. In the event of suspected or demonstrated noncompliance by an End User with the HMIS Security Awareness Agreement or any other HMIS plans, HMIS Policies and Procedures, HMIS

Data Quality Plan the Agency Technical Administrator/Contributory Agency security officer should notify the HMIS Team Lead via ticketing system to deactivate the User ID for the End User in question until an internal agency investigation has been completed. The HMIS Lead Agency shall be notified of any substantiated incidents that may have resulted in a breach of HMIS system security and/or client confidentiality, whether or not a breach is definitively known to have occurred.

4. 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 an Agency's access to HMIS for substantiated noncompliance with the provisions of these Security Standards, the San Antonio/Bexar County HMIS Policies and Procedures, or the Agency Privacy Statement that resulted in a release of Protected Health Information (PHI) which also encompasses Personally Identifiable Information (PII) and Personal Protected Information (PPI).

6. The HMIS Representative must submit and HMIS request to the HMIS ticketing system on behalf of a user whose account has been disabled due to inactivity, if the representative wishes to reactivate their account.

7. For accounts inactive for more than 180 days, the HMIS Representative may submit a refresher request to the HMIS help desk. These re-authorized users must attend and complete refresher training prior to reactivating their account.

8. For accounts inactive for more than 365 days, the HMIS Representative must submit a training request to the HMIS help desk. These re-authorized users must attend and complete new user training prior to reactivating their account.

Other Technical Safeguards

Most other technical safeguards for the San Antonio/Bexar County HMIS are currently implemented by the HMIS software vendor.

1. The HMIS Security and Compliance Coordinator shall develop and implement procedures for managing new, retired, and compromised HMIS account credentials.

2. The participating agency Security Officer shall develop and implement procedures that will prevent unauthorized users from connecting to private agency networks.

3. Unencrypted PPI may not be transmitted in any fashion—including sending file attachments by email or downloading reports including PPI to a personal flash drive

4. All physical documents containing PPI must be stored in a secure location.

4.13 SECURITY INCIDENTS

•The HMIS Lead must implement a policy and chain of communication for reporting and responding to security incidents.

•The participating agency and HMIS Lead will post the Privacy Notice anywhere HMIS data is collected or accessed that articulates the reporting mechanism for suspected breaches of client confidentiality. The notice will include contact information for the agency's HMIS Security Officer. The notice will include additional instructions for reporting anonymously.

•The participating agency and HMIS Lead will maintain records of all security incidents, responses and outcomes.

Reporting Security Incidents

These Security Standards and the associated San Antonio/Bexar 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 compromise of HMIS system security and/or client privacy must immediately report that possible incident to their Agency Security Officer. The participating agency security officer shall inform the HMIS Security and Compliance Officer.

2. In the event of a suspected security compromise participating 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 Agency

Security Officer should submit a request to the HMIS Lead to deactivate the End User's User ID until the internal investigation has been completed.

3. Following the internal investigation, the participating agency security officer shall notify the HMIS Security & Compliance Coordinator 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 HMIS Security and Compliance Coordinator reserves the right to permanently deactivate the User ID for the End User in question.

4. Within 1 business day after the HMIS Security & Compliance Coordinator receives notice of the breach, the HMIS Security & Compliance Coordinator and participating 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 Agency is not able to meet the terms of the action plan within the time allotted, the HMIS System Administrator, in consultation with the San Antonio/Bexar County Continuum of Care may elect to terminate the Agency's access to HMIS. The Agency may appeal to the HMIS Advisory Committee 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 Health Information (PHI) in noncompliance with the provisions of these Security Standards, the San Antonio 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 PHI in noncompliance with the provisions of these Security Standards, the San Antonio/Bexar County HMIS Policies and Procedures, or the Agency Privacy Statement.

8. The HMIS Lead Agency will maintain a record of all substantiated releases of PHI in noncompliance with the provisions of these Security Standards, the San Antonio/Bexar 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 an Agency's access to HMIS for substantiated noncompliance with the provisions of these Security Standards, the San Antonio/Bexar County HMIS Policies and Procedures, or the Agency Privacy Statement that resulted in a release of PHI.

4.14 SECURITY POLICY COMPLAINTS

•Complaints related to HMIS security policies and procedures will be considered using the same procedures for amending HMIS Documentation (see Section 1.5).

4.15 PROTECTED HEALTH INFORMATION STORAGE AND MANAGEMENT

•The safekeeping of clients' Personal Protected Information (PPI), which includes Protected Health Information (PHI), and Personally Identifiable Information (PII) and sensitive program information from unauthorized access, disclosure, use, or modification.

•Participating agencies and HMIS End Users are required to comply with federal, state and local confidentiality laws.

•Client information should only be searched and/or shared on a need-to-know basis.

4.15.1 ELECTRONIC DATA STORAGE AND MANAGEMENT

•System users may only store HMIS data containing PHI on devices owned by their agency.

•System users may not store HMIS data containing PHI on hard drives or removable media that can be accessed by non-system users.

•System users are responsible for safeguarding HMIS PHI that users store on agency-owned devices.

•Electronic transmission of HMIS data containing PHI will be limited to secure direct connections or, if transmitted over the internet, the data will be encrypted using a 128-bit key or transmitted using password protected files.

•The participating agency and HMIS Lead are responsible for developing additional policies and procedures for protecting electronic data from theft, loss, or unauthorized access.

•Before disposing of hard drives, USB drives, or other portable electronic media used to store PHI, the participating agency will consult with their agency HMIS Security Officer.

4.15.2 HARD COPY DATA STORAGE AND MANAGEMENT

•Hard copies of HMIS data containing PHI shall be kept in individual locked files or in rooms that are locked when not in use.

•When in use, hard copies of HMIS data containing PHI shall be maintained in such a manner as to prevent exposure of PHI to anyone other than the system user(s) directly utilizing the information.

•Employees shall not remove hard copies of HMIS data containing PHI from their agency's facilities without permission from appropriate supervisory staff unless the employee is performing a regular work function which requires the use of such records outside of the facility.

•Faxes or other printed documents containing PHI shall not be left unattended.

•Before disposing of hard copies of HMIS data containing PHI, they must be shredded.

•The participating agency is responsible for developing additional policies and procedures for protecting hard copies of HMIS data containing PHI from theft, loss, or unauthorized access.

4.15 AGENCY-SPECIFIC DATA SECURITY POLICIES AND PROCEDURES

•The participating agency may develop agency-specific data security policies and procedures that go beyond the standard polies included in this section.

•The participating agency is required to provide copies of agency-specific data security policies and procedures to the HMIS Security and Compliance Coordinator.

•The HMIS Security and Compliance Coordinator is responsible for reviewing agency-specific policies and procedures to determine if they conflict with the HMIS Policies and Procedures and resolving any conflicts.

•The participating agency is responsible for ensuring compliance with any agency-specific data security policies and procedures.

5. PRIVACY POLICIES

5.1 PURPOSE

•These privacy policies are meant to establish limitations on the collection, purpose, and use of data. It defines allowable uses and disclosures, including standards for openness, access, correction, and accountability. The policies provide protections for victims of domestic violence, dating violence, sexual assault, and stalking.

5.2 PRIVACY NOTICE

•The HMIS Lead will post a copy of the Privacy Notice on the HMIS website and will provide a copy of this document to any individual upon request.

•The participating agency must post a copy of the Privacy Notice at each workstation where client data is gathered and entered.

•The participating agency must also post a Spanish translation of the Privacy Notice, if it serves Spanish-speaking clients.

•Outreach workers inform clients about the Privacy Notice and provide a copy, if requested (including a copy of the Spanish translation, if applicable).

•The participating agency will post the Privacy Notice to its website, if one exists.

•The participating agency must state in the Privacy Notice that these privacy policies may be amended at any time and that amendments may affect information obtained by the agency before the date of the change.

•The participating agency should include in the Privacy Notice the contact information for their agency HMIS Security Officer for purposes of seeking additional information or submitting complaints.

•The participating agency must provide a copy of these Privacy Policies to anyone who requests it.

5.3 PURPOSE AND USE LIMITATIONS

•The participating agency and HMIS Lead may only collect and use HMIS data for the specific internal purposes relevant to the work of the Continuum of Care, as defined in this section. Every agency with access to Personally Identifiable Information (PII) must implement procedures to ensure and monitor its compliance with privacy policies and may only collect information by lawful and fair means with the knowledge and consent of the individual.

Authorized Uses of HMIS Data:

•To provide or coordinate services;

•To locate programs that may be able to assist clients;

•To produce agency-level reports regarding use of services;

•To track agency-level and CoC system-level outcomes;

•For agency operational purposes, including administrative functions such as legal, audits, personnel, oversight, and management functions;

•To comply with government and other funding agency reporting requirements;

•To identify service needs in our community;

•To support CoC system-level planning;

•To conduct research for government and educational purposes;

•To monitor compliance with HMIS Policies and Procedures; and,

•To accomplish any and all other purposes deemed necessary by the CoC Board.

5.4 INTERAGENCY DATA SHARING

•All client information entered in HMIS by the participating agency is shared with the agency's system users and with the HMIS Lead.

•With client consent, all client information is shared with system users at other participating agencies for authorized uses.

•The participating agency's Executive Director/Program Director (or equivalent) is responsible for their agency's compliance with the Interagency Data Sharing policies.

5.5 CLIENT CONSENT

Policies:

•The participating agency may infer client consent to collect and enter information into HMIS from any person who seeks or receives assistance from the agency.

•All information entered into HMIS is shared between the agency's system users and with the H4H as the HMIS lead, based on this inferred client consent model.

•In order to share information with other participating agencies, the agency must seek and obtain informed client consent using the Client Release of Information (ROI) form.

•When clients consent to share information, system users at other participating agencies will have access to the client's record and case history for authorized uses.

•Informed client consent is valid until such time as the client revokes consent.

•Clients who have consented to share information with other participating agencies may revoke consent in writing at any time. This revocation may impact other agencies' access to the client record and data they have entered into the system.

•The participating agency must store physical copies of client consent documentation.

Procedures (Initial Consent):

1. Personnel from the participating agency will notify the client that the information they collect will be entered into the HMIS and will explain the purposes for collecting information in the HMIS.

2. At this time, personnel from the participating agency will explain the Release of Information form, and the clients' right to revoke data sharing in writing at any time.

3. For families, an adult client can provide consent on behalf of household members by listing them in the spaces provided on the form and initialing in front of each family member's name. Additionally, the participating agency may seek consent separately from each individual in the household. A legal guardian (or another adult, if a guardian is not present) may sign on behalf of minors in the household.

4. The client will be provided the ROI form for review, will be explained its content, and will be asked to complete it.

5. The client must provide written consent using the ROI form as proof that they had an opportunity to review the form and have their questions answered. In the event that written consent is not feasible, a verbal or digital consent is permitted (i.e. on digital platforms, hotline, etc.), where the agency's personnel must read the privacy notice to the client before requesting the consent.

6. If the client signs the form and agrees to share information with all participating agencies, agency personnel must indicate their response in the HMIS.

7. If the client provides verbal consent, the agency personnel must indicate their response on the ROI "Verbal Consent Obtained" and retain a copy in the client's record.

8. If the client declines to share information with all participating agencies, agency personnel must ensure client indicts decision on the ROI, provide a copy to the HMIS Security and Compliance Coordinator and maintain a copy with client's documentation.

9. A copy of all completed consent forms will be kept in the client's paper file. These forms will be reviewed by the HMIS Security and Compliance Coordinator during security reviews.

Procedures (Revocation of Consent):

1. If a client presents a written request to revoke consent for information sharing in the HMIS, agency personnel must store the written request in the client's file, and must indicate their response in the HMIS.

2. If a client verbally requests to revoke consent for data sharing, agency personnel must ask the client to complete the ROI form and follow the process specified in (1) above.

3. A copy of all written ROI requests must be included in the client's paper file and uploaded in the individual's HMIS documents.

Procedure (Renewal of Consent):

If a client consents to share information after previously denying consent, agency personnel must follow the same procedures that were specified above involving the completion of the initial consent form.

5.6 ACCESS AND CORRECTION

• The participating agency must allow a client to inspect and to have a copy of any PHI about the client, and offer to explain information that the client may not understand.

• The participating agency must consider any request by a client for correction of inaccurate or incomplete PHI pertaining to that client. A participating agency is not required to remove any information but may, alternatively, mark information as inaccurate or incomplete and supplement it with additional information such as an indicator of data quality.

5.7 OTHER AUTHORIZED DATA DISCLOSURES

•Client data may be transmitted to reporting systems as mandated by agency funders.

•Other disclosures of client data to persons and organizations not authorized to view the information in the HMIS requires the client's written consent, unless the disclosure is required by law.

•Aggregated data that does not specifically identify any individual client or include PII may be shared with internal and external agents without specific permission.

5.8 ACCOUNTABILITY AND PRIVACY POLICY COMPLAINTS

•Complaints related to HMIS privacy policies and procedures will be considered using the same procedures for amending HMIS Documentation (described in Section 1.5).

•The participating agency must require each member of its staff to sign the Security Awareness Agreement.

6. QUALITY ASSURANCE POLICIES

6.1 PURPOSE

The purpose of quality assurance policies is to ensure reliable and useable data, establish expectations for participating agencies, and define quality standards.

6.2 POLICIES

•The HMIS Lead will develop a Data Quality Plan to assist participating agencies in maintaining and monitoring data quality.

•The HMIS Lead will define benchmarks and establish policies and procedures to monitor for compliance, including an enforcement mechanism for non-compliance.

•The HMIS Lead will include in the plan responsibilities for all parties.

•The participating agency must adhere to policies and procedures that ensure data meets standards for coverage, timeliness, completeness, accuracy, and consistency.

•The HMIS Lead will review the plan annually and update as needed.

6.3 STANDARDS

6.3.1 COVERAGE

The HMIS Lead seeks 100% participation in HMIS from all eligible homeless service providers and agencies within the CoC's geographic area, with a 60% minimum benchmark for both lodging (residential) and non-lodging (service-only) projects.

6.3.2 TIMELINESS

The participating agency is required to enter data into HMIS within 4 business days of client interview or interaction resulting in data collection.

6.3.3 COMPLETENESS

The participating agency is required to collect and enter data on 100% of those clients in participating projects.

6.3.4 ACCURACY

The participating agency is required to accurately represent in HMIS the information collected from clients and avoid entering misleading or knowingly false information. To accurately represent client information, the agency must follow data collection procedures.

6.3.5 CONSISTENCY

The participating agency must ensure personnel only use authorized data collection and entry procedures consistent with individual programmatic requirements.

Contributory HMIS Organization Agreement
("Agreement") For San Antonio / Bexar County
Continuum of Care
Homeless Information Management System Database
("HMIS")

HMIS is a client information system that provides a standardized assessment of the needs of those individuals that utilize social services related to homelessness ("**Clients**"), creates individualized service plans and records the use of housing and services which communities can use to determine the utilization of services of participating agencies, identify gaps in the local service continuum and develop outcome measurements. Agencies entering into HMIS must follow the HUD Data Standards, originally released in 2005 and last updated in 2019, and as revised from time to time ("**HUD Standards**") for entering in universal and program specific data elements. Haven for Hope ("**H4H**") is the HMIS lead agency and system administrator for the City of San Antonio and Bexar County.

Each agency that intends to access HMIS shall be considered a Contributory HMIS Organization ("**CHO**"). Prior to any representative of a CHO being given access to HMIS, the CHO shall sign and deliver this Agreement to H4H on an annual basis to indicate and reaffirm the CHO's responsibility to comply with the following provisions:

A. Confidentiality. In connection with its use of HMIS, the CHO shall comply with all relevant federal and state privacy and information security regulations and laws ("**Regulations**") that protect Clients' information ("**Client Information**") and shall only release Client Information in accordance with written consent of the Client, or as expressly permitted by the Regulations.

1. Subject to the requirements of the Texas Public Information Act, the CHO shall comply with the HMIS Privacy and Security Standards promulgated by HUD on July 30, 2004 at 69 FR 45927 (as revised from time to time) ("**HMIS Privacy Standards**"), and also the federal confidentiality Regulations in 42 CFR Part 2 regarding disclosure of alcohol and/or drug abuse records. In general terms, these Regulations prohibit the disclosure of alcohol and/or drug abuse records unless disclosure is expressly permitted by written consent of the person to whom it pertains or is otherwise permitted by 42 CFR Part 2.

2. The CHO shall not solicit or input information from Clients into HMIS unless it is essential to provide services; to conduct evaluations; for advocacy purposes, or as otherwise required or permitted by the HUD Standards. The CHO agrees not to release any Client Information received from HMIS to any organization or individual without the Client's express written consent (or as otherwise permitted by the Regulations). The CHO shall not enter into HMIS any data elements that are prohibited by law from being included in HMIS. However, for the purpose of avoiding duplication of individuals within HMIS, the CHO shall input universal data elements (e.g. name, date of birth, social security number) relevant to all service recipients regardless of whether information specific to the services is allowed to be input into HMIS.

3. The CHO shall ensure that all individuals affiliated with the CHO that are issued a User ID and password ("**Access Credentials**") for HMIS (each, a "**Representative**") receive basic user training provided by the H4H HMIS Department. The CHO shall ensure that its Representatives do not share Access Credentials with any other person or entity. The CHO shall inform the H4H HMIS Department as soon as possible, but no later than twenty-four (24) hours after the occurrence of any circumstances resulting in the need to deactivate a Representative's Access Credentials (e.g. if a user leaves the CHO's organization or otherwise no longer has a business need to access HMIS).

4. The CHO shall verbally explain to each Client the nature of the database prior to inputting any information into HMIS concerning the Client, and shall use reasonable efforts to obtain a written Release of Information in accordance with the HMIS Privacy Standards from each Client. The CHO will encourage Clients to participate in the collection of information.

5. The CHO shall be bound by all restrictions placed upon the data by any Client. The CHO shall diligently record in HMIS all restrictions requested. The CHO shall not knowingly enter false or misleading data under any circumstances, and shall correct any erroneous information upon becoming aware of the error.

6. If this Agreement is terminated, H4H and all other HMIS users shall continue to have the right to use all Client data previously entered into HMIS by the terminating CHO.

7. If a Client does not consent to sharing his or her information, only the Client's demographics should be entered into HMIS.

B. Use of Client Information and Data Entry.

1. The CHO shall only enter individuals in HMIS that exist as Clients within Bexar County or within other counties if required by the CHO, and the CHO has first obtained the written approval of the H4H HMIS Department.

2. The CHO shall use Client information in HMIS solely for the purpose of assisting the CHO in providing adequate and appropriate services to the Client.

3. The CHO shall consistently enter Client information into HMIS on a timely basis consistent with the HMIS Data Quality Plan as modified by the SARAH HMIS sub-committee from time to time.

C. Compliance; CHO's Indemnity; Limitation of Remedies.

1. The CHO shall ensure that its Representatives are bound by the same restrictions and conditions that apply to the CHO under this Agreement, and shall cause its Representatives to comply herewith.

2. The CHO shall use appropriate safeguards to prevent the unauthorized use or disclosure of Client Information in HMIS, and shall designate a security officer who implements information security

measures, ensures completion of Client Information privacy and security awareness training by Representatives annually, and conducts annual security reviews.

3. The CHO agrees to notify H4H as soon as possible upon becoming aware of any unauthorized access, use or disclosure of Client Information in HMIS, or any use of HMIS except as permitted by the HUD Standards.

4. **THE CHO HEREBY AGREES TO INDEMNIFY, DEFEND AND HOLD HARMLESS H4H AND ALL OTHER CHO'S (INCLUDING THEIR RESPECTIVE OFFICERS, DIRECTORS, EMPLOYEES, PROFESSIONAL ADVISORS, AND AGENTS) FROM AND AGAINST ALL DEMANDS, CLAIMS, SUITS, PROCEEDINGS, JUDGMENTS, SETTLEMENTS, ARBITRATION AWARDS, DAMAGES, LOSS, COST, EXPENSE (INCLUDING REASONABLE ATTORNEYS' FEES AND COSTS OF LITIGATION), SANCTIONS, FINES AND PENALTIES ARISING OUT OF OR RESULTING FROM ANY ACTS OR OMISSIONS OF THE CHO AND /OR ANY OF ITS REPRESENTATIVES IN VIOLATION OF THIS AGREEMENT**.

5. **NO PARTY SHALL BE LIABLE FOR ANY SPECIAL, INDIRECT, CONSEQUENTIAL OR PUNITIVE DAMAGES (INCLUDING LOSS OF PROFITS) UNDER OR IN CONNECTION WITH THIS AGREEMENT.**

D. TERMINATION; MISCELLANEOUS.

1. **EITHER PARTY MAY TERMINATE THIS AGREEMENT UPON THIRTY (30) DAYS WRITTEN NOTICE TO THE OTHER PARTY. IN ADDITION, EITHER PARTY MAY TERMINATE THIS AGREEMENT IF THE OTHER PARTY ("DEFAULTING PARTY") FAILS TO COMPLY WITH ANY OF ITS OBLIGATIONS UNDER THIS AGREEMENT AND SUCH FAILURE IS NOT CURED WITHIN SEVEN (7) DAYS AFTER THE DEFAULTING PARTY RECEIVES** a written notice of default from the other Party. Termination of this Agreement shall be without prejudice to any claims or obligations arising or accruing hereunder prior to the date of termination. Sanctions for violating this Agreement may include, in addition to any other remedies available at law or in equity, the requirement of additional training, the suspension/revocation of HMIS privileges, and the filing of criminal charges, if appropriate.

2. This Agreement may only be modified by a written amendment signed by both Parties. Waivers shall be express, written and signed by the Party bound thereby. There are no third party beneficiaries of this Agreement other than the indemnitees listed in paragraph C (4) above.

3. This Agreement shall be interpreted and enforced in accordance with the laws of the State of Texas without reference of conflicts of law's provisions. **Any dispute hereunder shall be brought exclusively in the state or federal courts located in Bexar County, Texas, and each Party agrees to waive its right to a trial by jury in any such proceeding**.

4. Notices shall be in writing and delivered by hand; facsimile, overnight courier, or certified or registered U.S. Mail, to the recipient's address below (or as modified in writing from time to time) and shall be deemed to be duly given when received on a business day (or the next following business day if the day of receipt is a non-business day).

IN WITNESS HEREOF, CHO has caused this Agreement to be executed by its duly authorized officer as of the Effective Date.

CHO Name: _____

Project Name(s): _____

By: _____

[Signature – Must be by the CHO CEO or Executive Director]

Name: _____

Title: _____

Effective Date: _____

HMIS Contact Information:	**CHO Contact Information**:
Attn.: David Huete 1 Haven for Hope Way, TC Bldg. #3-Administration San Antonio, TX 78207 Facsimile: (210) 220-2122 Email: david.huete@havenforhope.org Phone: (210) 220-2352 HMIS Security Officer: David Huete Phone: (210) 220-2352	Attn.: _____ Address: _____ _____ Facsimile: _____ Email: _____ Phone: _____ Security Officer: _____ Phone: _____

System Awareness Agreement

for the San Antonio / Bexar County Continuum of Care's Homeless Information Management System

HMIS is a client information system used to assess the needs of those individuals that utilize social services related to homelessness ("clients"), creates individualized service plans and records the use of housing and services, which communities can use to understand the utilization of services, identify gaps in the local service continuum and develop outcome measurements. Participating agencies and their system users must comply with the *HMIS Policies and Procedures*. Haven for Hope ("H4H") is the HMIS Lead Agency and serves as system administrator for San Antonio / Bexar County Continuum of Care ("CoC").

A. Confidentiality

I understand that I will be allowed access to confidential information and/or records in order to perform my specific job duties. I further understand and agree that I am not to disclose confidential information and/or records without the prior consent of the appropriate authority(s).

I understand that my User ID and Password to HMIS are issued for my use alone. I further understand that I am solely responsible for all information obtained, through system access, using my unique identification. At no time will I allow any other person to use of my account to access to HMIS. I understand that accessing or releasing confidential information and/or records, or causing confidential information and/or records to be accessed or released, on myself, other individuals, clients, relatives, etc., outside the scope of my assigned job duties would constitute a violation of this agreement. I understand my supervisor will be notified immediately of any violation and disciplinary action will be taken, up to termination of employment.

B. User Responsibilities

Users shall enter accurate, complete and timely data in accordance with the HMIS Policies and Procedures. **Please read each statement below and <u>sign your initials</u> to indicate you understand and accept the terms**.

___ My user ID and password are for my use only and must not be shared with anyone.

___ I will take reasonable measures to keep my password secure.

___ I understand that the only authorized users can view information in the system and the clients to whom the information pertains.

___ I will only access and use information that is necessary to perform my job.

___ If I am logged into the system and must leave my computer, I will first log out.

___ Any hard copies of electronic records will be kept in a secure file.

___ When hard copies are no longer needed, I will ensure they are properly destroyed.

___ If I notice or suspect a security breach or abuse of client confidentiality, I will immediately notify my HMIS Site Administrator or the HMIS System Administrator.

By affixing my signature to this document I acknowledge that I have been apprised of the relevant laws, concerning access, use, maintenance, and disclosure of confidential information and/or records which shall be made available to me through my use of the HMIS.

I further agree that it is my responsibility to assure the confidentiality of all information, which has been issued to me in confidence, even after my access to HMIS has ended. Pursuant to this agreement I certify that I have read and understand the laws concerning confidential information and/or records.

By signing the System Confidentiality and Use Agreement, you agree to comply with these terms and conditions. Failure to uphold these terms may result in loss of access or privileges.

USER NAME [PRINT]	DATE	AGENCY REPRESENTATIVE NAME [PRINT]	DATE
USER SIGNATURE	DATE	AGENCY REPRESENTATIVE SIGNATURE	DATE

Privacy Notice

for the San Antonio / Bexar County Continuum of Care's Homeless Information Management System

The U.S. Department of Housing and Urban Development (HUD) requires that each jurisdiction that receives funding from HUD have a Homeless Management Information System (HMIS) in place. This agency participates in the San Antonio / Bexar County HMIS administered by Haven for Hope (H4H), an electronic data collection system that stores information about the men, women, and children who access homeless and other human services in a community. The purpose of HMIS is to assist in determining your needs and to evaluate the effectiveness of services provided.

We only collect information that is needed to provide you services, or that we consider relevant to helping us understand the scope and dimensions of homelessness in order to design effective service delivery. We do not disclose your information without written consent, except when required by our funders or by law, or for specific administrative or research purposes outlined in our HMIS Privacy Policies. By requesting information and accepting services from this agency, you give consent for us to enter your information into the HMIS.

The collection and disclosure of all personal information is guided by strict security standards. You have the right to see your personal information collected by this partner agency and request changes if incorrect. A full copy of our agency's HMIS Privacy Policies is available upon request for your review.

Client Release of Information

for the San Antonio / Bexar County Continuum of Care's Homeless Information Management System

To provide you with the most effective and efficient service, we must collect relevant data for our Homeless Management Information System (HMIS). This secure and confidential database operated by trained representatives allows service providers to work together with you to make sure you are receiving the assistance you need in a timely manner. Beyond that, the HMIS allows the CoC to get an accurate count of all individuals experiencing homelessness or who are at risk of homelessness in San Antonio/Bexar County. To help us improve our current service system, coordinate services, and make plans for new services, we need to collect your personally identifiable information (PII). To better coordinate with other service providers, you have the right to consent to release your information to these other service providers.

Please review the information below and sign and date where indicated. *[Note to staff, if working with a family, please complete the back of this form as well].*

I understand and agree that this service provider will enter my information into the Homeless Management Information System (HMIS). The information I have provided is true and correct. I understand that my information may be shared among local service providers for the purpose of connecting me to services.

I understand that information about me that is in HMIS may be used by the service provider and the San Antonio / Bexar County Continuum of Care, including but not limited to, to conduct research and develop reports related to homelessness and housing programs, coordination of care, housing, service needs, income supports, education and employment, and program effectiveness. I authorize the collection of information, including PII, about the services provided to me and for this information to be included and shared with service providers in HMIS. I further understand that some of the information collected and shared may include records that are considered Protected Health Information under the Health Insurance Portability and Accountability Act (HIPAA). I understand that should I no longer want my information collected and shared, I may withdraw my consent in writing at any time by contacting: [Insert email address for Agency Security Officer]. Any information shared or collected prior to withdraw of consent cannot be revoked.

An agency representative has answered my questions about my privacy concerns. By signing this release form, I fully understand and agree to the above terms and conditions.

CLIENT NAME [PRINT]	DATE	CLIENT SIGNATURE	DATE

AUTHORIZED PERSONNEL NAME [PRINT]	DATE	AUTHORIZED SIGNATURE	DATE

Client Consent on Behalf of Household Members

An adult head of household may provide consent on behalf of family members to share their information in the HMIS.

FAMILY MEMBER NAME 1 [PRINT]	HEAD OF HOUSEHOLD [INITIALS]
FAMILY MEMBER NAME 1 [PRINT]	HEAD OF HOUSEHOLD [INITIALS]
FAMILY MEMBER NAME 2 [PRINT]	HEAD OF HOUSEHOLD [INITIALS]
FAMILY MEMBER NAME 3 [PRINT]	HEAD OF HOUSEHOLD [INITIALS]
FAMILY MEMBER NAME 4 [PRINT]	HEAD OF HOUSEHOLD [INITIALS]
FAMILY MEMBER NAME 5 [PRINT]	HEAD OF HOUSEHOLD [INITIALS]
FAMILY MEMBER NAME 6 [PRINT]	HEAD OF HOUSEHOLD [INITIALS]
FAMILY MEMBER NAME 7 [PRINT]	HEAD OF HOUSEHOLD [INITIALS]