Maricopa Regional CoC

HMIS Policies

2025

Maricopa Regional
Continuum of Care

TABLE OF CONTENTS

2025

MARICOPA HMIS COVERAGE PLAN

POLICIES & PROCEDURES

ADOPTED BY THE BOARD 04/25/2016

UPDATED BY THE BOARD 09/22/2025

Maricopa Regional
Continuum of Care

Overview

The Continuum of Care Interim Rule (24 CFR Part 578.7) delineates that the Continuum of Care is responsible for "…ensuring consistent participation of recipients and sub-recipients in the HMIS." This plan is written to outline the steps and responsible parties to ensure that this is taking place.

For questions or comments, please contact MAG Human Services at hsinfo@azmag.gov.

Participation and Outreach

Identification of Non-Participating HMIS Projects

Each year, with the support of the Collaborative Applicant (MAG) and the HMIS Lead (Solari), the Data Collaborative will form a workgroup to identify agencies that are suitable for HMIS, but not participating. This work will take place while preparing for the annual Housing Inventory Chart. The workgroup will complete this identification process by cross checking agencies in the 211 Resource Point with those in HMIS. Any agency on the 211 Resource Point list that is not in HMIS will be put on a list for outreach, which will be reviewed by the CoC Collaborative, MAG staff, and Solari staff for any additions.

Outreach to Non-Participating HMIS Projects

Once the list is finalized, the Collaborative Applicant, along with the HMIS Lead and volunteers of the CoC Collaborative and Data Collaborative, will outreach the identified agencies. The group will create standardized questions to ask agencies to find out any barrier keeping them from participating in HMIS. Extra emphasis will be given to projects that constitute a strategic priority of improving HMIS Bed Coverage or provide services to a strategic-population (i.e. veterans or youth). The group will establish responsible parties and outline the goal of bringing particular projects onto HMIS, if applicable. While standardized questions will be available, outreach to each agency should be customized to the needs of that agency. The outreach process should be time limited to no more than 60 days.

Report to CoC Board

The results of outreach efforts should be shared with the CoC Board on an annual basis for review and additional guidance.

2025

MARICOPA HMIS DATA QUALITY PLAN

POLICIES & PROCEDURES

ADOPTED BY THE BOARD 04/25/2016

UPDATED BY THE BOARD 10/28/2024

Maricopa Regional
Continuum of Care

Overview

Background

HMIS data quality refers to the reliability and comprehensiveness of the data recorded in the HMIS database. Good data quality results in better confidence that the data recorded in the HMIS accurately reflects the same information in the real world. Good data quality can "tell the story" of the population experiencing homelessness. The quality of data is determined by assessing characteristics such as ***coverage, utilization, completeness, accuracy, timeliness, and consistency.***

Objectives

The goal is to record the most accurate, consistent and timely information in order to draw reasonable conclusions about the extent of homelessness and the impact of homeless services.

Guiding Principles

Below are concise definitions of the six benchmarks of data quality that will be further described and defined in this document.

Coverage: The proportion of beds covered by the CoC's HMIS. High bed coverage rates indicate more accurate and reliable data.
Utilization: Program occupancy or the percentage of beds occupied on an average night.
Completeness: The degree to which HMIS records do not include partial or missing data. It also refers to the lack of data from projects not participating in HMIS.
Accuracy: Evident when the data in HMIS reflects the actual characteristics and experiences of clients. Inaccurate data significantly limits the ability of HMIS to serve as a tool in the community's effort to reduce homelessness.
Timeliness: The period between when client data is collected/known and when that information is entered into HMIS. Data not entered into HMIS shortly after it is known increases the potential for inaccuracies or errors in the data once it is in HMIS.
Consistency & Training: The degree to which the data is collected and stored in a uniform manner, across all users of the HMIS. Users that do not have a shared understanding of when, how, and why data should be collected in HMIS, are more likely to enter data that will not be accurate.

For questions or comments, please contact MAG Human Services at hsinfo@azmag.gov.

Data Quality Benchmarks

1. Coverage

- 100% of all HUD funded homeless assistance programs in Maricopa County will participate in the Maricopa HMIS.

- 100% of HUD Federal Partner homeless projects in Maricopa County will participate in the Maricopa HMIS.

- At least 85% of all beds in non-HUD funded residential homeless assistance programs located in Maricopa County will participate in the Maricopa HMIS

- Use the process in the HMIS Coverage Policy to determine what non-HUD funded projects need to be outreached and onboarded to ensure HMIS coverage.

2. Utilization

- 100% of the data entered into the Maricopa HMIS will accurately reflect bed utilization for the homeless projects in Maricopa County.

3. Completeness

- 98% of all clients entered will have complete HUD Universal Data Elements.
    - 2% is the maximum allowance for missing data, "Data not collected."
    - Outreach programs are exempt due to the nature of the work. Coordinated Entry Points may have up to 5% missing data.

- 95% of clients will have complete program data elements entered (should they be required).
    - 5% is the maximum allowance for missing data, "Data not collected."

- 95% of clients that exit will have data entered with exit destinations. Data not meeting this criterium is considered 'missing'.
    - Exit destinations are considered 'missing' when the response is either "Data not collected" or "No exit interview completed".
    - Additionally, within the 95% of exits with complete information, 5% is the maximum allowance for the responses of "Client doesn't know" or "Client refused".
    - Outreach and emergency shelter programs exempt due to the nature of the work.

- 5% additionally is the maximum allowance for "Client doesn't know" and "Client refused" responses of all answered questions.

- All programs that are required by federal partners to enter services must do so on a regular basis.

4. Accuracy

- As indicated in the HUD Data Quality Report Framework (Appendix A) the error rates for the following benchmarks shall not exceed:
    - 5% for Personally Identifiable Information (PII) (Q2)
    - 5% for Universal Data Elements (Q3)
    - 10% for Income and Housing Data Quality (Q4)
    - 5% Chronic Homelessness (Q5)
    - 5% Inactive Records: Street Outreach & Emergency Shelter (Q7)

5. Timeliness

- Client entry and exit records are entered within the following timeframes as indicated on the HUD Data Quality Report Framework (Q6):
    - **0-3 Days** for Coordinated Entry, Street Outreach, and Emergency Shelter.
    - **0-6 Days** for Transitional Housing, Permanent Supportive Housing, Rapid Re-housing, and Other Permanent Housing.

*It should be noted that some PSH and OPH projects may have client records that predate timeliness requirements.

6. Consistency & Training

The HMIS Lead will perform three types of regular training:

Regular New User Training: New user training is available live via web conference and recorded online and must be completed before a user is granted access to HMIS. Training is specific to each program's workflow.

Monthly Agency Administrator Training: Each program in HMIS is responsible for having a representative be responsible for the content in the monthly agency administrator training. This information may come in the form of a webinar or a newsletter. The webinar/newsletter will share important information that must be disseminated to users. It is at the discretion of the agency how programs will be represented. Some agencies may designate one representative while other agencies may select multiple representatives. Either way, the information must be shared with all users.

Refresher Training: From time to time, and at least annually, users are responsible for completing refresher trainings. The HMIS Lead is responsible for determining the content of the refresher trainings. Users must complete assigned refresher trainings within a 30-day window. If the user does not complete the training in the 30-day window, their user license will be subject to suspension.

Agencies should consider creating agency policy that outlines process for following the requirements outlined in each data quality benchmark.

HMIS Monitoring and Improvement Plan

Monitoring and enforcing data quality is a joint responsibility between agencies, the HMIS Team, the Maricopa CoC, and funders.

Agencies

Agencies are responsible for running their own data quality reports on each of their programs on a monthly basis. Each program should monitor their programs with three reports: the 0252 Data Completeness Report Card, the Data Quality Framework in ServicePoint, and a program specific performance report like the APR or CAPER.

HMIS Team

The HMIS team will conduct a monthly UDE Data Quality completeness audit. Any program which falls below the required UDE Data Quality completeness thresholds established will be notified and offered support on improving data quality. That support may come in the form of specific instructions to remedy errors or required training. If a program falls below the UDE Data Quality completeness threshold for three consecutive months, the HMIS Team will notify the Continuum of Care Data Collaborative about the concern. This notification will be made through the monthly performance reporting done by HMIS.

The HMIS team will also conduct a bi-annual review of agency Utilization and Timeliness. Utilization is a critical metric, which is closely tracked on the LSA and HIC. In addition, timeliness ensures the data agencies enter into HMIS is more accurate and reflective of reality. Solari will work with agencies on a bi-annual basis to help agencies better understand the gaps in their data quality.

The HMIS team will also present an annual report to the Data Collaborative showing the number of programs and agencies receiving notices of low data quality as well as an evaluation of data quality across the system. Information from these reports will be used to identify patterns in low quality and improve overall system data quality.

Data Collaborative

The Data Collaborative is responsible for supporting the HMIS Team and Agencies in enforcing the Data Quality Plan. Should an agency fall below the data quality thresholds and is unable to remedy the concerns with support of the HMIS Team, the Data Collaborative may take the following actions: recommend required training, provide notification to funders or the CoC Board, or recommend the agency's data entry be ceased until such a time their data quality can be improved.

On an annual basis, the Data Collaborative in collaboration with the HMIS team will complete an evaluation of data quality across the system to determine improvement plans. This process will include forming a workgroup to review data quality gaps in federal reporting (HIC/PIT, LSA, SPMs) and sending a survey to the community to gain an understanding of the data quality gaps in the field. Results of the report review and survey will be compiled and assessed for needed steps the CoC should take to improve data quality.

Funders

Funders of homeless programs are encouraged to hold programs accountable to the data quality plan by taking an active role in monitoring and enforcing data quality. This can be done by requiring the submission of standard data quality reports and the setting of minimum data quality thresholds as part of contract performance.

2025

MARICOPA HMIS PRIVACY PLAN

POLICIES & PROCEDURES

ADOPTED BY THE BOARD 04/25/2016

UPDATED BY THE BOARD 10/28/2024

Maricopa Regional
Continuum of Care

Overview

Background

The Continuum of Care Interim Regulation (24 CFR Part 578.7) describes that the Continuum of Care is responsible for reviewing, revising, and approving a **privacy plan, security plan, and data quality plan** for the HMIS. On July 30, 2004, the US Department of Housing and Urban Development (HUD) released the privacy and security standards for Homeless Management Information Systems (69 Federal Register 45888). This Privacy Plan is intended to be consistent with the HUD standards. All users, agencies and system administrators must adhere to this Privacy Plan.

We intend our Privacy Plan to support our goal of providing an effective and usable client support tool. We recognize that clients served by individual agencies are not exclusively that "agency's client" but instead are a client of the Maricopa County Continuum of Care. Thus, we have adopted a Privacy Plan which supports an open system of client-level data sharing amongst agencies whenever a client consents to do so.

Guiding Principles

The core tenant of our Privacy Plan is the Privacy Notice. The Privacy Notice describes how client information may be used and disclosed and how clients can get access to their information. Each agency must either adopt the baseline Privacy Notice or develop a Privacy Notice which meets and exceeds all minimum requirements set forth in the Privacy Notice (this is described in the Agency Responsibilities section of this Privacy Plan). This ensures that all agencies who participate in the HMIS are governed by the same minimum standards of client privacy protection.

Privacy Plan Document/Form	**Description**	**Use**
Maricopa Regional CoC Privacy Notice	This is the main document of this Privacy Plan. This document outlines the minimum standard by which an agency collects, utilizes, and discloses information.	Agencies must adopt a privacy notice which meets all minimum standards.
Maricopa Regional Continuum of Care Data Sharing ROI	This form notifies clients about the Privacy Notice and obtains their consent to share data within the HMIS.	Agencies must present an approved ROI to every client they serve that will be entered into HMIS.

List of Current Universal Data Elements & Participating Agencies	This outlines the list of shared data elements and agencies to whom those data elements are shared.	Agencies must be able to direct clients to this document.

For questions or comments, please contact MAG Human Services at hsinfo@azmag.gov.

Global Data Sharing

Data sharing of the Universal Data Elements among participating HMIS agencies began in 2013. Agencies participating in HMIS are expected to request client consent to share the HUD Universal Data Elements. In April of 2020, the Continuum agreed to expand the elements that are shared with all providers. The elements shared are any present on the Universal Data Elements (UDE) assessment. These fields include basic client demographic information, questions to determine chronicity, eviction information, housing-move in dates, and anything else approved by the Data Collaborative. Agencies which are prohibited from participating in data sharing (ex HOPWA, some RHY Programs) are exempt from this requirement. Agencies who have a legal justification for not requesting client consent to share the HUD Universal Data Elements may request an exemption from the Data Collaborative

Participating Agencies that are HIPAA covered entities, must adhere to the privacy and informed consent procedures as outlined in their internal processes and procedures. Further, these agencies have the responsibility of communicating with the HMIS Lead what data should not be shared per their requirements.

Visibility Group Sharing

Some agencies may need to share data based on a business need-to-know and coordination of care for sub-populations of individuals and families experiencing homelessness. These sharing practices based around affinity groups are called "Visibility Groups." This type of data sharing is in addition to the HUD Universal Data Element system-wide sharing.

The HMIS Lead has the discretion to approve or limit the number of visibility groups. Agencies wishing to form a visibility group must develop a data sharing Memorandum of Understanding (MOU) and provide that to the HMIS Lead. The MOU must include:

a. The agencies that agree to share data
b. A list of data elements that will be shared in addition to the standard Global sharing
c. The programs at each agency that will be entering the data. (Agreement must

note that data will be shared to the entire agency but that only certain programs may enter the data.)

d. A description of the consent process. What, if any, additional consent will be required from the client.
e. Identification of the key point people at each agency
f. Signatures from executive leaders

Verbal ROI

The collection of a client's consent via verbal ROI is permitted at the discretion of the Data Collaborative. Request for permission to use a Verbal ROI will be considered when:

a. There's a specified community or agency need, AND
b. The agency has a method to document the ROI, AND
c. The agency provides a verbal ROI script for the Data Collaborative to approve. (It is suggested that the verbal ROI follow the standard ROI template available from the HMIS Lead)

A verbal ROI will be approved on a per-program basis. Generally, an entire agency would not be permitted to collect a verbal ROI, as this accommodation should only be allowed for programs when necessary. Data Collaborative can approve a system-wide use of a verbal ROI under extenuating circumstances (e.g. public health emergencies).

Domestic Violence

The Violence Against Women Act (VAWA) and the Family Violence Prevention and Services Act (FVPSA) contain strong confidentiality provisions that limit the sharing of victims' personally identifying information, including entering information into public records and databases.

These provisions affirm confidentiality practices that protect the safety and privacy of victims of domestic violence, dating violence, sexual assault, and stalking. HMIS systems must protect the confidentiality of victims of domestic violence, dating violence, sexual assault and stalking seeking housing assistance. It requires that **both the HMIS and agencies** reasonably protect the identity of victims by refraining from disclosing personally identifying information.

Victim Service Providers (VSP) are agencies and programs designed specifically to provide services to victims of domestic violence, dating violence, sexual assault, and stalking. VSPs are **prohibited** from entering **PII** into HMIS.

User Responsibility

A client's privacy is upheld only to the extent that the users and direct service providers protect and maintain their privacy. The role and responsibilities of the user cannot be over-emphasized. A user is defined as a person that has direct interaction with a client or their data. (This could potentially be any person at the agency: a staff member, volunteer, contractor,

etc.)

Users have the responsibility to:

- Understand their agency's Privacy Notice and ROI
- Be able to explain their agency's Privacy Notice and ROI to clients
- Follow their agency's Privacy Notice
- Know where to refer the client if they cannot answer the client's questions
- Present the Privacy Notice and ROI to the client before collecting any information
- Uphold the client's privacy in the HMIS

Agency Responsibilities

The 2004 HUD HMIS Standards emphasize that it is the agency's responsibility for upholding client privacy. All agencies must take this task seriously and take time to understand the legal, ethical, and regulatory responsibilities. This Privacy Plan and the Privacy Notice provide guidance on the minimum standards by which agencies must operate if they wish to participate in the HMIS. Meeting the minimum standards in this Privacy Plan and the Privacy Notice are required for participation in the HMIS. Any agency may exceed the minimum standards described and are encouraged to do so. Agencies must have an adopted Privacy Notice which meets the minimum standards before data entry into the HMIS can occur.

Agencies have the responsibility to annually:

- Review their program requirements to determine what industry privacy standards must be met that exceed the minimum standards outlined in this Privacy Plan and baseline Privacy Notice (examples: Substance Abuse Providers covered by 24 CFR Part 2, HIPAA Covered Agencies, Legal Service Providers).
- Review the 2004 HUD HMIS Privacy Standards (69 Federal Register 45888)
- Adopt and uphold a Privacy Notice which meets or exceeds all minimum standards in the baseline Privacy Notice as well as all industry privacy standards. The adoption process is to be directed by the individual agency. Modifications to the Privacy Notice must be approved by the Data Collaborative.
- Ensure that all clients are aware of the adopted Privacy Notice and have access to it. If the agency has a website, the agency must publish the Privacy Notice on their website.
- Make reasonable accommodations for persons with disabilities, language barriers, or education barriers.
- Ensure that anyone working with clients covered by the Privacy Notice can meet the User Responsibilities.
- Designate at least one user that has been trained to technologically uphold the agency's adopted Privacy Notice.

System Administration Responsibilities (HMIS Staff)

HMIS Staff have the responsibility to:

- Adopt and uphold a Privacy Notice which meets or exceeds all minimum standards in the Privacy Notice.
- Train and monitor all users on upholding system privacy.
- Monitor agencies to ensure adherence to their adopted Privacy Notice.
- Develop action and compliance plans for agencies that do not have adequate Privacy Notices.
- Maintain the HMIS Website to keep all references within the Privacy Notice up to date.
- Provide training to agencies and users on this Privacy Plan.

2025

MARICOPA HMIS SECURITY PLAN

POLICIES & PROCEDURES

ADOPTED BY THE BOARD 04/25/2016

UPDATED BY THE BOARD 10/28/2024

Maricopa Regional
Continuum of Care

Overview

Background

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. These standards represent a minimum level of security required for all HMIS participating agencies.

For questions or comments, please contact MAG Human Services at hsinfo@azmag.gov.

HMIS Software Provider

The Maricopa HMIS uses the HMIS software provider's software. ServicePoint is supported by a very high system security including using 128-bit encryption, user authentication and user access levels.
The HMIS software provider employees, who have access to client-level data, are subject to a national background check, training on confidentiality requirements, and must sign a confidentiality statement as part of their employee agreement. The system function logs the time and type of activity, as well as the name of the user who viewed, added, edited, or deleted the information.

Servers are located in complexes with:

- Twenty- four (24) hour security personnel.
- Twenty- four (24) hour video surveillance.
- Dedicated and secured Data Center.
- Locked down twenty- four (24) hours per day.
- Only accessible by management-controlled key.
- No access is permitted to cleaning staff.
- State-of-the-art HVAC and fire suppression system.

Levels of User Access & Security

A licensed user is a person who has signed and submitted a Maricopa County HMIS Code of Ethics Agreement and completed basic user training. **Provider agencies are required to keep a physical or digital copy of the HMIS Code of Ethics Agreement on file at the agency for all current users.** Provider agencies are required to immediately deactivate users and inform the HMIS System Administrator if a user leaves an agency within 24 hours of their termination or departure by submitting a ticket to the HMIS Help Desk. In addition, users that do not actively use the system but retain a license pose a security risk. As a security measure, the HMIS team will audit the system once a month to determine which users have not logged in for 45 days or more. Notification will be sent to these users and the point-of-contact at their agency that if they do not login within a week following the notice, their user account will be deactivated.

HMIS staff will provide each user a unique username and initial password. Users are not to share usernames, as this is a breach of the Maricopa County HMIS Code of Ethics agreement and the HMIS Partnership Agreement. Exchanging usernames seriously compromises security and privacy of clients. If a breach occurs, it may subject the agency to discipline and termination of access to the Maricopa County HMIS system. HMIS conducts random audits of users to monitor that users are following the Maricopa HMIS Code of Ethics agreement.

HMIS Participating Agencies must establish an internal point of contact, known as the HMIS Primary Point of Contact, 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. Agency Leadership should be copied on the correspondence so that they are aware of new user requests. The Agency Administrator should encourage participating agencies to annually review the Maricopa County HMIS Code of Ethics agreement and the HMIS Partnership Agreement.

An agency must identify the type of user and programs each user should access within their agency.

Security Incident Procedures

All HMIS Participating Agencies and their authorized users must abide by the terms of all HMIS agreements. Failure to fulfill these agreements may result in immediate termination of HMIS access until issues are resolved. All breaches related to security must be reported to the HMIS Lead Agency immediately after 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 non-compliance with this policy that may leave HMIS vulnerable to intrusion or compromise client information. The HMIS Lead Agency and System 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 Administer who will notify the HMIS Lead Agency and System Administrator. Each HMIS Participating Agency will maintain and follow all procedures established by the HMIS Lead Agency, HMIS software, and Maricopa County Regional Continuum of Care Board related to thresholds for security incident reporting.

If an unauthorized entity were to gain access to the Maricopa County HMIS and client data, or if there is suspicion of probable unauthorized access/activity, HMIS, and the HMIS software provider will take immediate action to protect the security of the system. HMIS will comply with all applicable laws and work with the affected agencies to implement appropriate client notification.

Audit & Access Controls

The HMIS software provider maintains accessible audit trails that allows for the monitoring of user activity. They will also authenticate user activity via Internet Protocol address and present simultaneous user access.

All HMIS users are set up 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 their own unique user license.

Personal 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 each HMIS User:

- All passwords must be unique.
- All passwords must be rotated every 45 days.
- All passwords must be in a prescribed format recommending a mix of letters/numbers/capitalization/symbols.
- Upon the third unsuccessful login try, users will be locked out of the system. Users can select the "Forgot Password," option, request that their agency administrator reset their password or request that an HMIS administrator reset the password.
- All users with no login activity for at least 45 days will be notified of inactivity. If after one week, there is no further feedback from the user, they will be automatically deactivated.

Agency Administrators may reset passwords. If the Agency Administrator is unavailable or otherwise unable to reset a password for an end user, HMIS will reset a user's password in the event the password is forgotten. Users must request a password reset by submitting a request to the Maricopa County HMIS Help Desk at www.hmisaz.org. Password resets will only be sent to the agency provided email address.

Public Access Protocols

Program staff should be present to monitor workstations containing access to the HMIS database. Additionally, when workstations are not in use and staff is 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 database will automatically log the user out after 15 minutes of inactivity.

Users will ensure the confidentiality of client data, following all security policies in the Maricopa

County HMIS Policies and adhering to the standards of ethical data use, regardless of the location of the connecting computer. The Agency Administrator or designee has the responsibility to assure the user is in compliance with this and all other policies, procedures, agreements and rules governing the Maricopa County HMIS.

All users that access the Maricopa County HMIS remotely must meet the standards detailed in this document and may only access it for activities directly related to their job. Users may not access the system from unsecured networks (for example: coffee shops, restaurants, libraries and other public places).

Examples of allowable Remote Access:

- Personal laptops that were not purchased by the agency, if connected to a secured private network.
- Access to the Maricopa County HMIS on a secured private network other than that of the agency.
- Private home desktop, if connected to a secured private network.
- Use of mobile hotspots, if a secured private network.

If a user is found to have accessed the Maricopa County HMIS through an unsecured network, the user license will be immediately suspended.

Malware & 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 backup is conducted every 24 hours and is maintained using both power and alternative power systems at a different location from the primary HMIS servers.

Data Use

Client personal information exported from the system, either printed or electronic file types, poses a security risk. Client information should only be copied out of the secure HMIS database when necessary. Exported documents with client information are handled with care and are immediately destroyed after use, are stored in a locked area, or electronic files are stored in a secure location.

Agencies will dispose of personal information and remove personal identifiers not in current use seven years after the information was created or last changed.

Data Security and Encryption

The HMIS software provider ensures availability of customer data in the event of a system failure or malicious access by creating and storing redundant records. All data going across the Internet to the user's Web browser uses AES-256 encryption in conjunction with RSA 2048-bit key lengths.

The traffic that flows between the server and the user's workstation is encrypted using the SSL certificate installed on the HMIS software provider's dedicated servers. Database tape backups are performed nightly.

Tape backups are maintained in secure offsite storage. Seven (7) days' backup history is stored on instantly accessible storage. One (1) month's backup history is stored offsite. Users should report any experience of lag time or software down-time to the HMIS Help Desk by submitting a ticket. If system down-time occurs outside of the standard business hours, the users should contact the HMIS Manager or HMIS Director directly.

2025

MARICOPA HMIS NEW HMIS AGENCY

POLICIES & PROCEDURES

ADOPTED BY THE BOARD 04/25/2016

UPDATED BY THE BOARD 10/28/2024

Maricopa Regional
Continuum of Care

Overview

The purpose of this policy is to coordinate the process for new HMIS agency participation. All agencies who participate in the Maricopa Continuum of Care are encouraged to participate in the HMIS project to help promote coordination of care.

For questions or comments, please contact MAG Human Services at hsinfo@azmag.gov.

Procedure

The HMIS Lead Agency and the Continuum of Care Data Collaborative are responsible for determining if the new agency meets the requirements to participate in the Maricopa HMIS system.

HMIS Automatic Inclusion Criteria

- Solari provides initial review of the ticket and questionnaire within 3 business days.
- The CoC allows the HMIS Director/Manager to approve agencies that meet the following criteria:
    - The agency has a project dedicated to serving persons experiencing homelessness listed on the Maricopa County Housing Inventory Count (HIC) submitted annually to HUD;
    - The agency receives funding from HUD, another Federal Partner, or a local funder who requires participation in the HMIS database;
    - The agency will be participating in the Coordinated Entry process;
    - The agency is a funder (recipient) of a Federal Partner program grant which sub-contracts with local agencies (sub-recipient) which are required to use the HMIS. Access for these funders will be limited to contract monitoring activities. Access to client-level details must be granted by the local agency (sub-recipient).

HMIS Non-Automatic Inclusion Criteria

When agencies do not meet the automatic approval criteria, the Data Collaborative assesses the agency using the following 3 criteria.

1. The agency understands and states they can **meet all compliance requirements**.
2. The agency is **sufficiently part of the homeless services system** or program is sufficiently a homeless-serving program.
3. Agency Participation is **sufficiently a benefit to clients they serve, the agency, and the homeless service system** and CoC.

Agencies interested in participating in HMIS can complete a request form at https://community.solari-inc.org/submit-a-ticket/

Maricopa Regional Continuum of Care

HMIS Data Sharing Policy

2025

MARICOPA HMIS DATA SHARING

POLICIES & PROCEDURES

ADOPTED BY THE BOARD 04/25/2016

UPDATED BY THE BOARD 10/28/2024

Maricopa Regional
Continuum of Care

Objective

The purpose of the Data Sharing Policy is to outline the standardized process taken for each request to obtain and/or share the Maricopa Regional Continuum of Care's (CoC) HMIS data. This policy also includes the accompanying workflow for HMIS data requests and releases within the CoC.

Solari, Maricopa Association of Governments (MAG), the CoC Data Collaborative, and the CoC Board may place stipulations or conditions on data requests and releases as needed. Additional sharing of requested data, once provided to the requesting agency, is discussed on a case-by-case basis. All agencies that receive HMIS data will sign the Solari Data Sharing Agreement. Denial of data requests may be appealed to the CoC Board.

Maricopa HMIS data may be released from Arizona statewide HMIS warehouse known as DWEL-AZ and is not covered within this policy. Data releases from DWEL-AZ require approval from the DWEL Collaborative governance board of which Maricopa Regional CoC is a standing member with 3 designated representatives. Policies and procedures related to DWEL-AZ data sharing practices can be found at DWEL-AZ.org or by request to the DWEL-AZ Administrative Operator at dwel-az@solari-inc.org.

For questions or comments, please contact MAG Human Services at hsinfo@azmag.gov.

Guiding Principles

This combination of statements and questions guides the Data Collaborative and MAG in their decision-making process when reviewing a data request. This section is designed to be reviewed on an ongoing basis to ensure these principles align with CoC and community standards and needs.

Impact on System and Clients

- When assessing a data request, the Data Collaborative will consider all impacts the request could have on the system, paying special attention to impacts regarding those working in the system, clients, as well as any potential policy implications.

Sensitive Data

- Should a data request include sensitive data (e.g. domestic violence information, disability status, Personally Identifying Information, etc.), the Collaborative will consider the necessity of this information for the goal of the request, as well as assess impacts on the vulnerable populations the information refers to.
- All PII data requested will require CoC Board approval and will consider client impacts and/or improvement to client-level services.

Complexity and Capacity

- If Solari determines a request is complex, time-consuming, or will require a large capacity to fulfill, the Data Collaborative should discuss if the request is in alignment with CoC goals, contributes to service improvement, or otherwise benefits clients in the system. The request should also be assessed for its contribution to data-informed decision making, as opposed to a request made for the sake of curiosity.

Non-CoC Partner

- Requests from non-CoC partners will undergo additional assessment from the Collaborative to ensure both clarity of the request, as well as the requester's ability to accurately interpret CoC data. To further inform their decision, the Collaborative will utilize Solari's assessment of the estimated technical assistance needed if the requester is unfamiliar with the data.
- The Collaborative will assess the possibility of the requester's goals and findings aligning with CoC goals, and any subsequent opportunities for collaboration.

Broad or Unclear Scope

- Requests that include broader scope uses (i.e. ongoing requests for data) or unclear scopes will be evaluated on a case-by-case basis, likely asked to provide additional clarity, and offered initial approval for a one-time scope. Requesters will likely be asked to return to Data Collaborative with findings to be evaluated for an ongoing request based on the Collaborative's analysis. Approved ongoing requests will be considered for reevaluation on a regular basis for the findings' relevancy to CoC goals and policies.

Data Quality Impacts

- Request will be assessed for the level at which data quality concerns may impact findings of the request.
- If needed, a data quality disclaimer will be added. Should a disclaimer be added to the request, the requester will be required to display or announce the disclaimer on any findings.

Audience Consideration

- Data Collaborative will assess the intended audience for the findings of the request (e.g. general public, city council, academia, etc.) and factor this into the approval decision.
- If restrictions of information sharing are needed, a disclaimer will be provided to the requester.

Data Request Workflow

The Maricopa Regional Continuum of Care HMIS Data Request Form is completed when an agency or organization needs access to data that is not readily available or part of a required report. Common examples of these requests include:

- Client-level data outside of the organization requesting
- Research requests
- Advanced data analysis
- Statewide or aggregate data that is not publicly accessible

The Maricopa Regional CoC HMIS Data Request Form is intended to help the CoC prioritize and make decisions on the denial or approval of data requests. The data requests process can be started by first submitting a ticket at https://community.solari-inc.org/submit-a-ticket/.

Solari and MAG are responsible for determining what data is released and what approvals are needed prior to releasing data. The following data request workflow informs the process of determining the level of approval required:

Requester:

- Complete Data Request Form with all required fields.
- Dependent upon the nature of the request, the requester may be expected to maintain open communication with the Data Collaborative, MAG, or Solari on data analysis progress prior to publication of findings or results.
- Unless otherwise noted, requester is expected to share the final results with the CoC either by providing the final report or providing a basic presentation of results. This is to ensure that value derived from the data is used to benefit clients and service agencies who provided the data.

Solari:

- Review request within 3 business days of submission.

- Provide a compliance and logistics report to MAG for processing. Report will include:
  - Compliance with HMIS Policies (Including Privacy, Security, DQ)
  - Narrative response on HMIS Technical Support needed
  - Narrative response on the proposed uses outlining any concerns
  - Time estimates for completing work
  - Approximate delivery date outlining competing priorities
  - Proposed data use concerns
  - Cost estimate, if necessary

MAG:

- Review request within 2 business days of receiving compliance and logistics report from Solari.
- Determine appropriate path for request from the following options:
  - Deny request based on CoC and HMIS policy.
  - Approve requests for aggregate level data that is non-complex and limited in scope. Examples include:
    - HUD Required Reports
    - Federal Partner Reports
    - Common Demographic Reports
    - Existing system-wide aggregate reports
    - Analysis of CoC-Approved Dashboards
    - Analysis / addition query into existing reports
  - Bring requests that do not fall in the above two categories to Data Collaborative for deliberation.
- Depending on the above determination, MAG will respond directly to the Requester with approval, denial, or next steps to bring the request to Data Collaborative.
- MAG and Solari will work together to maintain internal tracking of data requests to ensure consistency and standardization of data releases.

CoC Data Collaborative:

- Data Collaborative will use the Data Sharing Policy's Guiding Principles to assess each data request.
- All requests involving personally identifying information (PII) will also require CoC Board approval.
- For data requests that include larger policy implications, the Data Collaborative may seek additional Board approval.

CoC Board:

- Act on recommendation provided by the Data Collaborative based on the guiding principles in the Data Share Policy.

The final decision on a request will come from MAG within a month, depending on the need for CoC Data Collaborative and CoC Board approval.

2025

MARICOPA HMIS RELEASE OF INFORMATION & PRIVACY NOTICE

POLICIES & PROCEDURES

ADOPTED BY THE BOARD 04/25/2016

UPDATED BY THE BOARD 10/28/2024

Maricopa Regional
Continuum of Care

HMIS ID Number: _____

Maricopa Regional Continuum of Care HMIS Release of Information

The Maricopa Regional Continuum of Care authorizes agencies to utilize a common and shared data system called the Homeless Management Information System (HMIS) to work together to provide services for those experiencing homelessness. The benefit of sharing your client information is that it will allow us to assist in planning for and providing services to you, the client. This information will be shared among agencies to coordinate and deliver your services. Know that passwords, encrypted technology, or other means protect all information entered in these databases. Steps are taken to safeguard the information that is entered into the system, but no system is infallible.

Provider agencies work together and share detailed information about their clients through databases that track your services. Any provider agency using these systems requires all database users to sign an agreement to keep their information confidential and use it only for program purposes. You are not required to permit your information to be shared to receive services. There are many benefits to sharing your personal information with other providers. We may be able to provide you with more housing options and placement in housing may be quicker if we can coordinate with other agencies. In addition, it will save you from having to repeat information to multiple service providers when accessing services. In addition to the benefits of sharing information, there are risks. The risks include that some sensitive information about the diagnosis or treatment of a mental health disorder, drug, or alcohol disorder, HIV, AIDS, or domestic violence concerns may be shared to connect you with appropriate services.

The following data elements will be shared:

- Personal identifying information such as name, Social Security Number, and date of birth
- Demographic information such as race, ethnicity, and gender
- Information about you that may help in locating housing resources such as veteran status or whether you or a member of your family has a disabling condition.
- Information about your history of housing and homelessness such as where you have been living and where we can reach you.
- Information about services you have received through other homeless providers.

Additional client information will be shared only with certain agencies to assist in coordinating services. Attached is a list of data elements that will be shared as well as which agencies will be sharing information.

HMIS ID Number: _____

Other agencies may join the HMIS collaboration in the future. Signing this ROI allows for the sharing of data not only with current agencies but agencies that may join in the future. An updated list can be found at https://community.solari-inc.org/homeless-management-information-system/

By signing this form, I acknowledge and agree to the following:

- I have received a copy of The Privacy Notice, which describes how the primary identifying information and other client data information may be used or disclosed.
- I have the right to ask questions about this form and anything that I do not understand about data sharing.
- **I have the right to opt out of having information shared with other participating agencies and still receive services from that agency.** I am still eligible for services if I do not consent to data sharing, but it may limit the coordination available.
- I have the right to change my consent to share.
    - If I later **agree to share**, all information previously not shared will now be available to all agencies using HMIS.
    - If I later **decide not to share**, I understand that the data previously entered will still be available to the agencies it was originally shared with. New information collected by this agency will not be shared.

If applicable, this ROI also applies to all non-adult members of my household. I agree to share my information and the information of my family members listed below.

Names and Dates of Birth: (Attach separate page if necessary)

Mark Below if you do not want to have your information shared in HMIS.

	I DO NOT AGREE to share my information. **Your information will be shared in HMIS unless you check this box **

_____

Client Signature Date

_____

Client Printed Name

_____

Staff Signature Date

_____ _____

Agency Staff Printed Name Agency Printed Name

Maricopa Regional CoC Privacy Notice

THIS NOTICE DESCRIBES HOW INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

A. What This Notice Covers

1. This notice describes the privacy policy and practices of [Name of Agency]**.** Our central office is at [Address, web address, telephone contact information**.]**
2. If this agency operates programs that are covered by HIPAA laws, additional privacy information will be provided and supersedes the information in this Privacy Notice.
3. Our agency and many others participate in the Maricopa Regional Continuum of Care (CoC). The CoC promotes and funds communitywide goals and programs to end homelessness and utilizes data to make informed decisions.
4. The Maricopa Regional CoC has approved the use of various data systems for the collection and sharing of personal information including a computer system called a Homeless Management Information System (HMIS). The CoC may approve additional data systems for community use in the future.
5. When a person requests or receives services from this agency or other agencies participating in the CoC, information about them and members of their household will be entered into these computer systems. These computer systems will be used by multiple agencies.
6. The policy and practices in this notice cover the processing of Protected Personal Information (PPI) of this and other agencies utilizing the approved data systems of the CoC. All personal information that the agencies maintain, not just the information entered into the data system, is covered by the policy and practices described in this notice. This policy covers only the programs within the agency that participates in HMIS.
7. Protected Personal Information (PPI) is any information we maintain about a client that:
    a. allows identification of an individual directly or indirectly
    b. can be manipulated by a reasonably foreseeable method to identify a specific individual, **or**
    c. can be linked with other available information to identify a specific client. When this notice refers to personal information, it means PPI.
8. We adopted this policy to provide accurate information about how your data may be used and to comply with the privacy standards for Homeless Management Information Systems (HMIS) and all CoC-approved databases. We intend this policy and practices to be consistent with the standards of 69 Federal Register 45888 (July 30, 2004).
9. This notice tells our clients, our staff, and others (such as our funders, the CoC, and other social services providers) how we process personal information. We follow the policy and practices described in this notice.
10. We may amend this notice and change our policy or practices at any time. Amendments may affect personal information that we obtained before the effective date of the amendment. All amendments are approved by the CoC Board. Current information about the CoC Board can be found at the MAG website www.azmag.gov/Committees/.

11. We give a written copy of this privacy notice to any individual who asks. We maintain a copy of this Privacy Notice on the HMIS website: https://community.solari-inc.org/homeless-management-information-system/.
12. The HMIS is administered by Solari Crisis & Human Services. Their office is at 1275 West Washington Street, Suite 210, Tempe, AZ, 85281. Their website is https://community.solari-inc.org/homeless-management-information-system/. You can contact the system administrator at 602-908-3605.
13. The agency to contact regarding the CoC is the Maricopa Association of Governments located at 302 N. 1st Avenue, Phoenix, AZ 82003. Their phone number is 602-254-6300.

B. How and Why, We Collect Protected Personal Information

1. We collect personal information only when appropriate to provide services or for another specific purpose of our agency or when required by law.
2. We may collect personal information for these purposes:
   a. To provide or coordinate services to clients.
   b. To locate other programs that may be able to assist clients.
   c. To verify information given to us by clients
   d. For functions related to payment or reimbursement from other services that we provide
   e. To operate our agency, including administrative functions such as legal, audits, personnel, oversight, and management functions
   f. To comply with reporting obligations
   g. To improve services on a system level
   h. When required by law
3. We may be required to collect some personal information by law or by organizations that give us money to operate this program. Other personal information that we collect is important to run our programs, improve services, and better understand the needs of individuals in the community. We only collect information necessary to coordinate and deliver services.
4. We only use lawful and fair means to collect personal information.
5. We collect personal information with your knowledge and consent. If you seek our assistance and provide us with personal information, we verify your consent to the collection and processing of that information as described in this notice.
6. We may also get personal information, with your consent, from:
   a. Individuals who are you have identified as part of your household
   b. Individuals who you have identified as assisting you
   c. Individuals or organizations you provide for verification of information or references
   d. Information already collected about you by other agencies that are part of the HMIS
   e. Other private organizations in the CoC
   f. Government agencies and their data systems including Regional Behavioral Health Authority
   g. Public records including internet searches, telephone directories, and other published sources
7. We post a sign at our intake desk or other location explaining the reasons we ask for personal information. The sign gives our agency's contact information and the location of this privacy notice.

C. How We Use and Disclose Protected Personal Information

1. We use or disclose PPI for activities described in this part of the notice. **We may or may not make any of these uses or disclosures with your information.** We share client records with other agencies that may have separate privacy policies and that may allow different uses and disclosures of the information.
2. All participating agencies of the CoC share personal client information. The information that is shared with participating agencies may include all information you have provided or has been obtained with your consent. The list of these agencies and the information shared are subject to change. You will be asked to sign a Release of Information to disclose your PPI upon consent. The Release of Information document provides specific details of how your information will be shared in the CoC data systems.
3. Agencies use and disclose data pertinent to the services and data collection requirements. Each agency must execute a partnership agreement with the administrator of the data system outlining the proper use of the system. All users of the system are required to abide by a code of ethics.
4. **You have the right to opt out of having information shared with other participating agencies and still receive services from that agency.** If you opt out of sharing your information, your information will remain in the data system(s) and be subject to the other disclosures in this privacy notice, but the information will not be available to the other participating agencies. If you opt out of sharing your information, that decision may change what additional resources or agencies are available to you. We share data with our partners, including payers like AHCCCS, public benefit agencies, and administrative partners to assist with eligibility determinations, care coordinators, and social services outreach.
5. By signing the Release of Information, you consent to the use or disclosure of your PPI for the purposes described here:
   a. to provide or coordinate services
   b. for functions related to payment or reimbursement for services
   c. to carry out administrative functions such as legal, audits, personnel, oversight, and management functions
   d. to create de-identified (anonymous) information that can be used for research and statistical purposes
   e. when required by law to the extent that use, or disclosure complies with and is limited to the requirements of the law
   f. to avert a serious threat to health or safety if
      (1) we believe that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public, and
      (2) the use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat
   g. to report an individual, we reasonably believe to be a victim of abuse, neglect, or domestic violence to a governmental authority (including a social service or protective services agency) authorized by law to receive reports of abuse, neglect, or domestic violence
      (1) under any of these circumstances:
         (a) where the disclosure is required by law and the disclosure complies with and is limited to the requirements of the law
         (b) if the individual agrees to the disclosure, or
         (c) to the extent that the disclosure is expressly authorized by statute or regulation, and

(I) we believe the disclosure is necessary to prevent serious harm to the individual or other potential victims, or

(II) if the individual is unable to agree because of incapacity, law enforcement or other public official authorized to receive the report represents that the PPI for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual can agree to the disclosure.

(2) when we make a permitted disclosure about a victim of abuse, neglect, or domestic violence, we will promptly inform the individual who is the victim that a disclosure has been or will be made, except if:

(a) we, in the exercise of professional judgment, believe informing the individual would place the individual at risk of serious harm, or

(b) we would be informing a personal representative (such as a family member or friend), and we reasonably believe the personal representative is responsible for the abuse, neglect, or other injuries, and that informing the personal representative would not be in the best interests of the individual as we determine in the exercise of professional judgment.

h. for academic research purposes

(1) conducted by an individual or institution that has a formal relationship with this agency if the research is conducted either:

(a) by an individual employed by or affiliated with the organization for use in a research project conducted under a written research agreement approved in writing by a designated agency program administrator (other than the individual conducting the research), or

(b) by an institution for use in a research project conducted under a written research agreement approved in writing by a designated agency program administrator.

(2)) any written research agreement:

(a) must establish rules and limitations for the processing and security of PPI during the research

(b) must provide for the return or proper disposal of all PPI after the research

(c) must restrict additional use or disclosure of PPI, except where required by law

(d) must require that the recipient of data formally agree to comply with all terms and conditions of the agreement, and

(e) is not a substitute for approval (if appropriate) of a research project by an Institutional Review Board, Privacy Board, or other applicable human subjects' protection institution.

i. to a law enforcement official for a law enforcement purpose (if consistent with applicable law and standards of ethical conduct) under any of these circumstances:

(1) in response to a lawful court order, court-ordered warrant, subpoena, or summons issued by a judicial officer, or a grand jury subpoena

(2) if the law enforcement official makes a written request for PPI that:

(a) is signed by a supervisory official of the law enforcement agency seeking the PPI

(b) states that the information is relevant and material to a legitimate law enforcement investigation

(c) identifies the PPI sought
(d) is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought, and
(e) states that de-identified information could not be used to accomplish the purpose of the disclosure.

(3) if we believe in good faith that the PPI constitutes evidence of criminal conduct that occurred on our premises
(4) in response to an oral request to identify or locate a suspect, fugitive, material witness, or missing person the PPI disclosed consists only of name, address, date of birth, place of birth, Social Security Number, and distinguishing physical characteristics, or
(5) the official is an authorized federal official seeking PPI for the provision of protective services to the President or other persons authorized by **18 U.S.C. 3056**, or to foreign heads of state or other persons authorized by **22 U.S.C. 2709(a)(3),** or for the conduct of investigations authorized by **18 U.S.C. 871 and 879** (threats against the President and others), and the information requested is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought.

j. to comply with reporting obligations
k. to the administrators, vendors, and contractors of the CoC-approved data systems
l. to Data Warehouse Enterprise for Linkage Arizona (DWEL-AZ) for purposes of state-wide coordination of services and academic research purposes. More information is available at DWEL-AZ.org.

6. Before we disclose your personal information that is not described here, we seek your consent.

D. <u>How to Inspect and Correct Protected Personal Information</u>

1. You may inspect and have a copy of your PPI that we maintain. We will offer to explain any information that you may not understand.
2. We will consider a request from you for the correction of inaccurate or incomplete personal information that we maintain about you. If we agree that the information is inaccurate or incomplete, we may delete it or we may choose to mark it as inaccurate or incomplete and supplement it with additional or corrected information.
3. To inspect, get a copy of, or ask for correction of your information, ask a program staff member how to obtain this information.
4. We may deny your request for inspection or copying of personal information if:
   a. the information was compiled in reasonable anticipation of litigation or comparable proceedings
   b. the information is about another individual (other than a health care provider or homeless provider)
   c. the information was obtained under a promise of confidentiality (other than a promise from a health care provider or homeless provider) and if the disclosure would reveal the source of the information, **or**
   d. disclosure of the information would be reasonably likely to endanger the life or physical safety of any individual.
5. If we deny a request for access or correction, we will explain the reason for the denial. We will also include, as part of the personal information that we maintain, documentation of the request and the reason for the denial.
6. We may reject repeated or harassing requests for access or correction.

E. Data Quality

1. We seek to maintain only personal information that is accurate, complete, and timely.
2. We will dispose of personal information and remove personal identifiers not in current use seven years after the information was created or last changed.
3. We may keep information for a longer period if required to do so by statute, regulation, contract, or other requirements.

F. Complaints and Accountability

1. If you would like to submit a complaint regarding HMIS, you may contact the Solari Crisis & Human Services Compliance Department to initiate a formal investigation. To do so, please call 844-852-4287 or email Compliance@solari-inc.org.
2. All members of our staff (including employees, volunteers, affiliates, contractors, and associates) with access to personal information are required to comply with this privacy notice. Each staff member must receive and acknowledge receipt of a copy of this privacy notice.
3. Questions or complaints about the agency serving you should follow the agency's grievance procedure. Questions or complaints that are broader than the services of a single agency or the use of a single data system can be directed to the CoC. If you are unsure where to go, you may go to any agency listed below and we will help you determine the best person to speak with.

[AGENCY CONTACT INFORMATION]

HMIS System Administrator: Solari Crisis & Human Services
1275 West Washington Street, Suite 210
Tempe, AZ, 85281
602-908-3605
https://community.solari-inc.org/homeless-management-information-system/

Continuum of Care Information: Maricopa Association of Governments
302 N. 1st Avenue
Phoenix, AZ 82003
www.azmag.gov
602-254-6300

G. Change History:

1. April 2016 – Adopted HUD's baseline privacy notice and approved by the CoC Board.
2. May 2018 – Minor revisions to update contact information and grammar.
3. January 2022 - Minor revisions to update contact information.
4. June 2022 – Update to reflect AHCCCS notes.
5. May 2024 - Minor revisions to update grammar and new approved agencies.

Maricopa Regional Continuum of Care Data Collection

Agencies participating in the Maricopa Regional Continuum of Care are asked to collect some client data to provide services and assist in the housing of clients. The following data is collected by all participating agencies. Data collected by one agency may be shared with other agencies in the HMIS.

Identifying Information	Demographic Information	Homeless History	Service & Housing Information
Name Social Security Number Veteran Status Date of Birth AHCCCS ID Photo Household Relationships Zip Code of Last Address	Race Ethnicity Gender Disabilities	Reason Homeless Times Homeless Dates of Homelessness Type of Prior Residence City of Prior Residence	Dates Served by Program City Housed Date Housed

Maricopa Regional Continuum of Care Participating Agencies

The Maricopa Regional Continuum of Care has participating agencies throughout the county of Maricopa. The following agencies currently participate in the HMIS and may potentially share data throughout the system. New agencies participating in the HMIS will be added to this list.

Agency	City	Website
A New Leaf	Mesa	http://www.turnanewleaf.org
Andre House of Arizona, Inc.	Phoenix	http://www.andrehouse.org
Area Agency on Aging, Region One	Phoenix	https://www.aaaphx.org/
Arizona Behavioral Health Corporation	Phoenix	http://www.azabc.org
Arizona Complete Health – Complete Care Plan	Tempe	https://www.azcompletehealth.com/
Arizona Department of Economic Security	Phoenix	https://des.az.gov
Arizona Friends of Foster Children Foundation	Phoenix	https://www.affcf.org
Arizona Housing Inc.	Phoenix	http://www.azhousinginc.org
Arizona Pet Project	Phoenix	https://azpetproject.org/
Arizona Youth Partnership	Tucson	http://www.azyp.org
Atlas Medical Systems	Phoenix	https://atlasmeds.com/
AZCEND	Chandler	http://azcend.org
Banner University Health Plans–Complete Care Plan	Phoenix	https://www.bannerufc.com/acc
Basic Mission	Laveen	None
BCBS Health Choice	Phoenix	https://www.healthchoiceaz.com/
Beia's Families	Phoenix	https://beiasfamilies.org/
Carry Me Productions	Tempe	www.carrymeproductions.org
Catholic Charities Community Services	Phoenix	http://www.catholiccharitiesaz.org
Central Arizona Shelter Services	Phoenix	http://www.cassaz.org
Center for Health and Recovery	Phoenix	https://azchr.org/
Chicanos Por la Causa	Phoenix	http://www.cplc.org
Child Crisis Arizona	Phoenix	https://childcrisisaz.org/

Circle the City	Phoenix	http://www.circlethecity.org
City of Avondale	Avondale	https://www.avondaleaz.gov/
City of Chandler	Chandler	https://www.chandleraz.gov/
City of Glendale	Glendale	https://www.glendaleaz.com/
City of Mesa	Mesa	https://www.mesaaz.gov
City of Phoenix	Phoenix	https://www.phoenix.gov
City of Tempe	Tempe	https://www.tempe.gov/
Community Bridges	Mesa	http://communitybridgesaz.org
Community43	Phoenix	https://community43.org
COPA Heath	Mesa	https://copahealth.org/
dehp Therapeutics	Phoenix	https://dehpcare.com/
Family Promise of Greater Phoenix	Scottsdale	http://www.familypromiseaz.org
Foster Arizona	Mesa	https://fosterarizona.org
Homeless ID Project	Phoenix	http://www.azhomeless.org
Homeless Youth Connection	Avondale	http://www.hycaz.org
House of Refuge	Mesa	http://www.houseofrefuge.org
Human Services Campus	Phoenix	http://www.hsc-az.org
Justa Center	Phoenix	https://www.justacenter.org/
Keys to Change (HSC/LDRC)	Phoenix	https://hsc-az.org/
La Frontera Arizona	Tucson	http://www.lafronteraaz.org
La Mesa Ministries	Gilbert	https://www.lamesaministries.org
Lifeology	Phoenix	https://wearelifeology.com/
Lutheran Social Services of the Southwest	Phoenix	http://www.lss-sw.org
Molina Complete Care Plan	Phoenix	https://www.molinahealthcare.com/members/az/en-us/mem/medicaid/medicaid.aspx
Maggie's Place	Phoenix	http://www.maggiesplace.org
Maricopa Association of Governments	Phoenix	http://www.azmag.gov
Maricopa County	Phoenix	https://www.maricopa.gov
MercyCare	Phoenix	https://www.mercycareaz.org
The Mercy Center of Arizona	Phoenix	https://www.mercycenterofarizona.com/
Mercy House	Phoenix	https://www.mercyhouse.net/
Mesa United Way	Mesa	https://www.mesaunitedway.org/
National Community Health Partners	Tucson	https://www.nchponline.org/
Native American Connections, Inc.	Phoenix	http://www.nativeconnections.org
Novum Health	Phoenix	https://www.novumhealth.com/
One n Ten	Phoenix	http://www.onenten.org
Open Hearts Family Wellness	Phoenix	https://openheartsaz.org/
Phoenix Rescue Mission	Phoenix	http://www.phoenixrescuemission.org
Phoenix VA Health Care System	Phoenix	http://www.phoenix.va.gov

Project Veteran's Pride	Glendale	http://pvpjwh.org/
Resilient Health	Phoenix	https://resilienthealthaz.org
Save the Family Foundation of Arizona	Mesa	http://www.savethefamily.org
Society of Saint Vincent de Paul Diocese of Phoenix	Phoenix	http://www.stvincentdepaul.net
Southwest Behavioral & Health Services	Phoenix	http://www.sbhservices.org
St. Joseph the Worker	Phoenix	https://sjwjobs.org/
Streets of Joy	Phoenix	https://www.streetsofjoy.com/
Tempe Community Action Agency, Inc.	Tempe	http://www.tempeaction.org
Tempe Fire Medical Rescue	Tempe	http://www.tempe.gov/fire
Terros Health	Phoenix	https://www.terroshealth.org/
The Salvation Army Phoenix Social Services	Phoenix	http://www.salvationarmysouthwest.org
The Salvation Army Tempe Corps	Tempe	http://www.salvationarmytempecorps.org
UMOM New Day Centers	Phoenix	http://www.umom.org
United Healthcare	Phoenix	https://www.uhc.com/
US Vets	Phoenix	http://www.usvetsinc.org/phoenix
Veterans 5-9	Phoenix	https://veterans5-9.com/