



MARICOPA HMIS

POLICY AND PROCEDURES

PREFACE

Maricopa Homeless Management Information System

Overview

Congress has established a national goal that all communities should be collecting an array of data about homelessness, including unduplicated counts of individuals who are homeless, their use of services and the effectiveness of local assistance systems. In order to achieve this objective, the Department of Housing and Urban Development (HUD) encouraged communities to develop a Homeless Management Information System (HMIS) and has provided funding through the Supportive Housing Program, Continuum of Care process to assist in the implementation of systems to collect this data.

Background

The Maricopa HMIS implementation began with a community wide planning process in December 2001. The Maricopa Association of Governments, on behalf of the Continuum of Care Regional Committee on Homelessness and the Community Information & Referral, Inc. (CI&R) of Maricopa County, convened a planning process to identify the high level requirements for the Maricopa Homeless Management Information System (HMIS) and to select a software vendor that would meet the requirements of the local community and the U.S. Department of Housing and Urban Development (HUD). Community Information & Referral is the Grantee and host agency for implementation of the Maricopa HMIS. This planning process, which included representatives of homeless provider agencies, city, county and state government agencies, private foundations, and private information technology experts, developed a design for the system and presented its recommendations to the Continuum of Care Regional Committee on Homelessness and its Planning Subcommittee for approval.

Following the approval, the planning participants developed a Request for Proposals, identified potential software vendors, and issued a public invitation to bid on the requirements. The resulting recommendation, also approved by the Continuum of Care Regional Committee on Homelessness and its Planning Subcommittee, was that the CI&R enter into negotiations with Bowman Internet Systems, LLC for ServicePoint, and contract for co-location of the servers and database with Bowman Internet Systems.

The creation and implementation of the Maricopa HMIS could not have become a reality without the support of six funding partners: The Lodestar Foundation, The Arizona Department of Housing (formerly The Governor's Office of Housing Development), The Arizona Community Foundation, The Virginia G. Piper Charitable Trust, The Valley of the Sun United Way, and the Maricopa Association of Governments/AZ Department of Economic Security. Local funds were utilized for both the planning and implementation phases of project.

Implementation

The Maricopa HMIS implementation structure includes a User Group, an Advisory Board and the Continuum of Care Regional Committee on Homelessness through its Planning Subcommittee.

The User Group is responsible for oversight of the implementation, development of policies and procedures and problem resolution regarding system implementation. This serves as a forum for current and future users to discuss their implementation status, raise questions and participate in the policy setting process.

The Maricopa HMIS Advisory Board which is comprised of community, local government, business and agency stakeholders provides advice and guidance regarding the overall implementation of HMIS and serves as a forum for key stakeholders to be provided information about the implementation of HMIS, to participate in the planning and policy setting, to assist in fund raising and to understand the potential of HMIS implementation.

The Continuum of Care Regional Committee on Homelessness and its Planning Subcommittee monitors the implementation of HMIS and serves as the final decision maker for issues that are not resolved at the User Group or CI&R Director Level.

The Project Team, comprised of the CI&R Director and representatives of Symmetric Solutions, Cannon & Associates (providing planning, facilitation and oversight services) and TechSelect Consulting (providing web services, and financial services) meet on a bi-weekly basis to review implementation status, plan next steps, resolve outstanding issues and ensure the Project stays on track.

The Maricopa HMIS Policy and Procedures Manual was developed by the HMIS Users Group. They are designed to support implementation and ongoing use of the System to ensure strict client confidentiality, security of information and consistent application of the functions provided by *ServicePoint*. The User Group and the Project Team will continue to update these Policies and Procedures as needed.

For information regarding the implementation of the Maricopa HMIS contact the project web site at www.cir.org/hmis or Community Information and Referral at 602-263-8845.

Roberto Armijo
Executive Director
Community Information & Referral Services Inc.

This Policy & Procedures Manual may be copied in part or in full when due acknowledgement is provided to the Maricopa HMIS.

Table of Contents

GLOSSARY OF TERMS	1
I – ROLES AND RESPONSIBILITIES	1
<i>Agency & Stakeholder Involvement</i>	2
II – DATA AND SYSTEM INTEGRITY	1
<i>Database Access and Data Entry</i>	2
<i>Local Data Storage</i>	14
<i>Virus Control Management</i>	15
<i>Monitoring Provider Agency Compliance</i>	17
<i>Corrective Action Plan</i>	24
<i>Risk Assessment and Disaster Recovery – Pending</i>	28
<i>Data Quality Assurance</i>	29
III – PRIVACY AND CONFIDENTIALITY	1
<i>Maintenance of Client Confidentiality</i>	2
IV – SOFTWARE SUPPORT	1
<i>Hours of System Operation</i>	2
<i>Technical Support</i>	4
<i>Rapid Response Technical Support</i>	6
V – TRAINING REQUIREMENTS.....	1
<i>Training Requirements – To be Developed</i>	2
VI – REPORT GENERATION	1
<i>Reports</i>	2
VII – SOFTWARE DEVELOPMENT	1
<i>Data Conversion – To Be Developed</i>	2
<i>Data Integration – To Be Developed</i>	3
<i>Design Changes – To Be Developed</i>	4
<i>Software Testing – To Be Developed</i>	5
VIII – SYSTEM HARDWARE.....	1
<i>Hardware Acquisition</i>	2
<i>Hardware Replacement – To Be Developed</i>	4
<i>User Workstation Standards</i>	5
IX – MARKETING AND GROWTH	1
<i>Application for Admission to HMIS – To Be Developed</i>	2
<i>Public Relations – To Be Developed</i>	3
APPENDICES	1
<i>Appendix A: Agency Profile Form</i>	2

<i>Appendix B: Client Acknowledgement of Data Entry into the Maricopa Homeless Management Information System</i>	5
<i>Appendix D: Computer Security Incident Report</i>	6
<i>Appendix E: Corrective Action Plan Format</i>	8
<i>Appendix F: Custom Report Request Form</i>	9
<i>Appendix G: Agency Reports</i>	11
<i>Appendix H: Systemwide Reports</i>	12
<i>Appendix I: Hardware Request Form</i>	13
<i>Appendix J: HMIS Code of Ethics</i>	15
<i>Appendix K: Rescinding Client Consent</i>	17
<i>Appendix L: Audit Reports</i>	18
<i>Appendix M: Standard Data Requirements</i>	19

GLOSSARY OF TERMS

1. *Anonymous client*: A client entered into the database with a unique computer generated identifying code acting as a reference for that client.
2. *Client*: Any person who received, applied for or was denied services by a Provider Agency.
3. *Client Identifying Information*: Any information or a combination of data that would allow an individual client to be identified including but not limited to name, nick name, social security number, military identification number, health insurance carrier number.
4. *ClientPoint*: A module of ServicePoint that allows users to enter, edit, view, or print client information. ClientPoint offers sophisticated features such as building and tracking family relationships, restricting client records, and conducting case management.
5. *Client's guardian*: Any person legally responsible for a minor or an adult, according to Arizona Revised Statutes (A.R.S.). All references to "client" in this policy also apply to "client's guardian."
6. *Close to real-time*: Data entry within one business day.
7. *Computer virus*: A self-replicating piece of computer code, which resides in active memory and partially or fully, attaches itself to files and/or applications.
8. *Computer worm*: Similar to viruses, worms reside in active memory of computers and replicate themselves and will usually interfere with normal computer use or a computer program. Unlike viruses, worms exist as separate entities and do not attach themselves to other files or programs.
9. *Consultation*: A discussion, usually by phone, reminding the End-user or Provider Agency, of proper security and/or confidentiality practices(s), following confirmed inappropriate action(s).
10. *Custom Report*: A report, which can be created by HMIS Provider Agencies using the ServicePoint Report Writer.
11. *Deficiency*: An insufficiency in the software application.
12. *End-user*: Any person given access to the database including staff and volunteers.
13. *Error*: A documentable occurrence that prevents an end-user from proceeding further.
14. *Firewall*: A system or group of systems that enforces an access control policy between two networks. The system may contain a pair of mechanisms: one that exists to block Internet traffic, and the other that exists to permit Internet traffic.
15. *HMIS Provider Database*: A software application, which allows HMIS staff to track all communication relating to Provider Agencies.
16. *Malicious code*: An illegitimate computer code, which produces an undesired effect including Trojan horses, viruses and worms.
17. *Maricopa HMIS database*: The Homeless Management Information System's database, also know as HMIS database and/or database.
18. *Outside source(s)*: Organization(s) who are not current HMIS Provider Agencies.
19. *Performance*: The lack of execution and/or operation of the software.
20. *Probation*: A trial period of time, not greater than one hundred and eighty days (180), in which an End-user or Provider Agency addresses and corrects inappropriate actions(s).
21. *Provider Agency*: An agency authorized to participate in the Maricopa County Homeless Management Information System.

22. *Quality of Data Issue*: Any concern that decreases the accuracy and completeness of the data as defined by the Minimum Data Requirement.
23. *Real-time*: Immediate data entry upon seeing a client.
24. *Reinstatement Corrective Action Plan*: A modified Corrective Action Plan developed specifically for the purpose of preparing and assessing the appropriateness of reinstating a previously terminated Agency as an HMIS Provider Agency.
25. *ResourcePoint*: A module of ServicePoint that allows for adding, editing, classifying, locating agency, program, and service data by city, state, county, zip code or keyword search options. Also allows printing of agency location maps and publication of the resource database to a publicly accessible web site or printed directory.
26. *Restricted client*: A client whose name is known by only the entering Provider Agency, HMIS System Administrator II, and those agencies the client grants access to his/her name.
27. *Sanctions*: Penalties for noncompliance specified by the HMIS User Group and CI&R Executive Director.
28. *Self-replicate*: Makes copies of itself.
29. *ServicePoint*: A web-based information management system for service providers of an agency, coalition or region of any size which provides client tracking, case management, agency and program indexing, and reporting – all in a real-time environment.
30. *ShelterPoint*: A module of ServicePoint that allows viewing of shelter availability, checking clients in and out, and referral or making of reservations for clients to shelters.
31. *Suspension*: An act of postponing database access, after an End-user or Provider Agency receives written notice via certified mail explaining a breach of contract, quality of data issue or improper security and/or confidentiality practices, where the guilty party received previous warning(s) and did not correct inappropriate actions.
32. *Technical Support Staff*: Include, in ascending order, Help-desk personnel, Application Specialist, HMIS System Administrator and Bowman Internet System's Help desk personnel.
33. *Termination*: The act of ending database access, after an End-user or Provider Agency receives an appropriate written notice via certified mail explaining the reasons for cessation of database use.
34. *Trojan horse*: A malicious, security-breaking program, which pretends to be a benign application such as a screen saver, a game, or some other valuable program; but purposefully causes something the user does not expect. Unlike a virus, Trojan horse do not replicate, but Trojan horse programs attacks pose one of the most serious threats to computer security.
35. *Written Warning*: A printed notice informing the End-user or Provider Agency of a confirmed inappropriate action and a corrective explanation of the desired conduct.

I – ROLES AND RESPONSIBILITIES

Agency & Stakeholder Involvement

Policy: Maricopa Homeless Management Information System (HMIS) implementation and ongoing operations provides agency and stakeholder involvement at all levels to ensure broad community participation.

Purpose: To define participants' roles and responsibilities in Maricopa HMIS.

Scope: System wide

Definitions: *End-user:* Any person given access to the database including staff and volunteers.

Provider Agency: An agency authorized to participate in the HMIS.

Procedure:

1.0 HMIS ADVISORY BOARD

1.1 Established according to the following guidelines:

- Comprised of all stakeholders including client and client advocate representatives, shelters, advocacy organizations, and governmental agencies.
- Includes the Executive Director or designee of each Provider Agency.

1.2 Responsibilities:

- Assists with fundraising and resource development.
- Encourages client, service provider, and community involvement.
- Oversees quality assurance and accountability.
- Assists CIR on guiding principles for Community Information & Referral, Inc. (CIR), Provider Agencies, and client participation with regard to HMIS implementation.
- Oversees security and confidentiality in the HMIS Policy and Procedures manual.

2.0 HMIS USER GROUP

2.1 Comprised of voluntary, non-paid positions:

- Provider Agency representatives (Majority membership)
- Funders and reporting agencies (Minority membership)
- CIR representative
- HMIS Project Team (staff support to the User Group)

2.2 Responsibilities:

- Provides policy and technical assistance to CIR
- Assists in development of:
 - 1) Quality and timing of provider training
 - 2) Policies and procedures
 - 3) Common system documents and reports
 - 4) Information sharing agreements

- 5) Decisions on data access by external parties
- 6) Minimum data elements
- 7) Common assessments and picklists
- 8) Soliciting feedback from all End-users about proposed system changes
- Serves as a Review and Appeal body, in regards to Provider Agency violations and grievances.
- Assist CIR in developing and implementing HMIS marketing to other providers.
- Communicates with and encourages attendance by representatives of the cities of Phoenix, Scottsdale, and Tempe, as well as, the Arizona Department of Economic Security/Community Services Administration, the Arizona Department of Health Services/ Division of Behavioral Health, and the Arizona Development of Housing.
- Assists in defining criteria, standards, and parameters for releasing aggregate data.
- Oversees security and confidentiality in the HMIS Policy and Procedures manual.

3.0 CONTINUUM OF CARE REGIONAL COMMITTEE ON HOMELESSNESS (CoC)

3.1 The CoC oversees the CIR management of the HMIS in Maricopa County.

3.2 Responsibilities:

- Receives periodic HMIS related reports from CIR.
- Assesses impact of these reports on overall HUD funding to the CoC.
- Receives and processes CIR requested continuation of HMIS HUD funding.
- Assists CIR and Provider Agencies to identify and apply for other public and private funding sources for HMIS operations.
- Provides general direction for major changes in the HMIS operation, participants (Provider Agencies), and End-users.
- Receives and approves HMIS system-wide information and reports.

4.0 HMIS ADMINISTRATOR (CIR)

4.1 As the recipient of the HUD funds and other matching funds and the legal contractor for access to the software, CIR oversees implementation, management, and maintenance of the Maricopa HMIS.

4.2 Responsibilities:

- Works in partnership with the CoC Planning sub-committee and Provider Agencies.
- Hires the HMIS Project Manager
- Responds to community questions about the homeless community.
- Identifies and applies for public and private funds, in conjunction with HMIS User Group and the CoC Planning sub-committee, to continue HMIS future operation.

5.0 HMIS PROJECT MANAGER

5.1 Administration

- Reports fund expenditures and HMIS project outcomes to HUD.
- Acquires HMIS software, which meets HUD requirements.
- Oversees the preparation of a detailed HMIS implementation plan and schedule.
- Oversees the HMIS Project Team.
- Provides staff support to the HMIS User Group.
- Develops and implements, with the User Group, marketing the HMIS to other providers.

5.2 Database

Oversees Bowman Systems project performance:

- Responds to system needs on an on-call basis, 24 hours a day as needed to implement disaster recovery plan.

5.3 Implementation

- Advises Provider Agencies of implementation schedule.
- Works with System Administrator and each Provider Agency to identify implementation issues.
- Prepares implementation plan for each agency along with System Administrator.
- Attends Project Team meetings.
- Communicates all aspects of implementation with CIR Executive Director.

5.4 Training

- Oversees all training of Provider Agency administrators and End-users.

5.5 Support

- Oversees Help-Desk function.
- Oversees Bowman Systems technical support services.
- Supervises internal and external security protocols.
- Addresses HMIS technical operational issues.

5.6 Data integrity

- Monitors operation of the HMIS database.
- Monitors and evaluates the quality, timeliness, and accuracy of data input, data management, and data reports.
- Assists HMIS User Group and Advisory Board.
- Identifies and addresses potential operational issues with individual Provider Agencies, the HMIS User Group, the CoC Committee, and the State Evaluation Project.

5.7 Reports

- Oversee system-wide reporting.
- Oversee reporting documentation.

6.0 HMIS SYSTEM ADMINISTRATOR

6.1 Implementation

- Advises Provider Agencies of implementation schedule.
- Works with each Provider Agency to identify implementation issues.
- Prepares implementation plan for each Provider Agency.

6.2 Training

- Oversees training of Provider Agency End-users in the operation of the HMIS.
- Assists with HMIS-related technical issues.

6.3 Support

- Assists with Help-Desk function by providing level 2 technical support.
- Supervises internal and external security protocols.
- Assists with backup and disaster recovery.
- Addresses HMIS technical operational issues.
- Helps with technical assistance with Provider Agency sites.

6.4 Data integrity

- Monitors operation of the HMIS database.
- Monitors and evaluates the quality, timeliness, and accuracy of data input, data management, and data reports.

- Addresses issues with individual Provider Agencies and HMIS User Group.
- Helps ensure integrity and reliability of HMIS information.
- Identifies and addresses potential operation issues with individual Provider Agencies, and the HMIS User Group.
- Monitors functionality, speed, and database backup procedures of SQL Server 2000 database.

6.5 Reports

- Assists with Provider Agencies and Report Writer Specialist in report development.
- Works closely with Agency Administrators to develop queries.
- Documents work on the database and development of reports/queries.

7.0 REPORT WRITER SPECIALIST

7.1 Responsibilities:

- Writes detail report specifications based on requests from the User Group and Project Team.
- Generates reports using Advanced Reporting Tool (ART).
- Understands and operates reporting tools such as Excel, Crystal Reports and others.
- Develops documentation of created reports.

8.0 HELP-DESK COORDINATOR

8.1 Responsibilities:

- Maintains toll-free Help-Desk.
- Provides level 1 technical assistance and trouble-shooting
- Documents questions, issues, problems, and suggestions.
- Reports the above to System Administrator monthly and quarterly.
- Coordinates on-site training.
- Updates the HMIS training manual.

9.0 PROVIDER AGENCY EXECUTIVE DIRECTOR OR DESIGNEE

9.1 Each Provider Agency Executive Director may choose an Agency Administrator to administer the following responsibilities. If there is not a designated Executive Director, these tasks fall to the Agency Administrator.

9.2 Responsibilities:

- Assumes responsibility for integrity and protection of client information entered into the HMIS database.
- Establishes and ensures business controls and practices which will adhere to the HMIS Policies and Procedures.
- Develops and maintains **internal** policies and procedures to ensure:
 1. New and continued staff training.
 2. Timely and accurate input of HMIS data.
 3. Personnel procedures addressing violations of the HMIS Code of Ethics.
 4. Protocols for data access and reporting.
- Communicates security and confidentiality requirements to End-users.
- Monitors End-user compliance in regards to security, confidentiality, and data integrity.
- Is responsible for insuring appropriate use of the database by Provider Agency's designated staff.
- Allows HMIS database access only to qualified End-users based upon job description and need to access.

- Addresses HMIS concerns with CIR and User Group in a timely and professional manner.
- Implements client grievance and appeals procedure in relation to HMIS database.

10.0 AGENCY ADMINISTRATOR

10.1 Each Provider Agency appoints one person as their Agency Administrator.

10.2 Responsibilities:

- Edits and upgrades agency profile information on ResourcePoint
- Creates User-name and computer generated password for personnel authorized to access the system by the Provider Agency's Executive Director.
- Assures new staff training on the HMIS System.
- Reviews Maricopa HMIS Policies and Procedures with all End-users, both new and old.
- Reviews security and confidentiality of client information with authorized staff.
- Allows access to the HMIS System only after the authorized End-users completes all necessary training and signs documents outlined in End-user Training Guide.
- Notifies all agency End-users of interruptions in service.
- Attends or supplies representation to User Group meetings.
- Updates Provider Agency and End-users on decisions made during User Group meetings.
- Administers Provider Agency specified business and data protection controls.
- Administers and monitors access to HMIS database.
- Provides 24-hour technical support assistance to agency's End-users.
- Provides assistance during backup and recovery of data to HMIS technical support and HMIS System Administrator.
- Provides a manual data entry processes in the event of a HMIS disaster.
- Identifies and reports Policies and Procedures violations to the User Group and System Administrator.

11.0 END-USER

11.1 **CIR's End-user access:** only those parties authorized for the following reasons may be provided access to the HMIS:

- Technical administration of the database (System Administrator(s), Project Manager, and Help-Desk Assistance)
- Report writing
- Data analysis/entry/correction
- Report Generation
- Back-up or server maintenance
- ResourcePoint updates.
- Other essential activities associated with carrying out HMIS-related responsibilities.

11.2 The **Provider Agency End-user access:** only those parties authorized for the following reasons may be provided access to the HMIS:

- Data entry
- Editing Client records
- Viewing Client records
- Report writing
- Administration
- Other essential activities associated with HMIS Provider Agency business use.

11.3 Responsibilities of **ALL** End-users:

- Adhere to HMIS and Provider Agency Policy and Procedures.
- Protect HMIS and Provider Agency data and information.
- Prevent unauthorized disclosure of data.
- Report Security Violations to Agency Administrator.
- Remain accountable for all actions undertaken with his/her End-user name and password.

II – DATA AND SYSTEM INTEGRITY

Database Access and Data Entry

Policy: Provider Agencies regulate and monitor End-user access and data entry into the Maricopa Homeless Management Information System (HMIS).

Purpose: To provide guidelines to Provider Agencies about database access and data entry.

Scope: All HMIS Provider Agencies and Agencies' End-users.

Definitions:

Client: Any person who received, applied for, or was denied services by a Provider Agency.

Client's guardian: Any person legally responsible for a minor or an adult, according to Arizona Revised Statutes (A.R.S.). All references to "client" in this policy also apply to "client's guardian."

Close to real-time: Data entry within one business day.

End-user: Any person given access to the database including staff and volunteers.

Maricopa HMIS database: The Homeless Management Information System's database, also known as HMIS database and/or database.

Provider Agency: An agency authorized to participate in the HMIS.

Restricted client: A client whose name is known by only the entering Provider Agency, HMIS System Administrator II, and those agencies the client grants access to his/her name.

Real-time: Immediate data entry upon seeing a client.

Unnamed client: A client entered into the database with a unique computer generated identifying code acting as a reference for that client.

Procedure:

1.0 PROVIDER AGENCY'S RESPONSIBILITIES

1.1 HMIS Database Access

Provider Agency will

- Sign HMIS Agency Participation Agreement.
- Set up End-user identification and grant access to the database based upon the End-user's job description.
- Never transmit End-user identification and computer generated password together in one e-mail, fax, telephone call or other means of communication. They must be transmitted separately (e.g. one portion via e-mail and the other via voice) unless physically handed to the

End-user, who must destroy the paper transmission upon successfully entering the HMIS database.

- Delete an End-user including the Agency Administrator immediately at the termination of his/her employment or a change in job duties/position.
- Notify HMIS System Administrator when the Agency Administrator is leaving the Agency Administrator position.
- Notify the HMIS System Administrator of new Agency Administrator's name two weeks prior to terminating current Agency Administrator OR Notify the HMIS System Administrator, as soon as possible, in the event of an immediate Agency Administrator discharge.
- Identify and establish access parameters for End-user work terminals.
- Notify HMIS System Administrator of access parameters for End-user work terminals.

1.2 Security

Provider Agency will:

- Monitor End-user access to the HMIS database. (See Appendix for End-user Access Report samples)
- Provide periodic reviews of security procedures. (See Appendix for Audit Reports)
- Assume responsibility for staff and End-user's compliance with security.
- Notify the designated Agency Administrator or the HMIS System Administrator immediately of any suspected security breach.

1.3 Data

1.3.1 Consent Form

Provider Agency will:

- Provide client consent form(s) as required by the Provider Agency, state, and/or federal laws and the Maricopa HMIS standards.
- Provide, in its original form or modified for the specific agency, the HMIS Client Acknowledgement of Data Entry into the Maricopa Homeless Management Information System form to permit sharing of confidential client information to other HMIS Provider Agencies.

1.3.2 Data Entry

Provider Agency will:

- Assume responsibility for End-user's data entry and accuracy.
- View, obtain, disclose, or use the database information only for business purposes related to serving the Provider Agency's clients.
- Monitor End-user data entered into the HMIS database, in accordance with Provider Agency's policies and the Maricopa HMIS minimum data standards.
- Not delete a client profile created by another Provider Agency.
- Correct inaccurate information and missing required data elements.

- **Not** misrepresent the number of clients served or the types of services/beds provided.

1.4 HMIS Activity Participation

Provider Agency will:

- Designate a staff member to regularly attend HMIS User Group meetings and to communicate HMIS updates, HMIS policy and practice guidelines, HMIS data analysis, HMIS software/hardware upgrades, and HMIS decisions to Provider Agency.
- Designate a staff member as the HMIS Agency Administrator, who will attend specific training for this position.
- Update virus protection software on agency computers that accesses the HMIS database on a scheduled, regular basis.

1.5 Legal Parameters

Provider Agency will:

- Not transmit any material in violation of United States federal or state law which includes, but is not limited to: copyright material, material legally judged to be threatening or obscene, and material considered protected by trade secret.
- Not use the Maricopa HMIS with intent to defraud the federal, state, or local government or an individual entity, or to conduct any illegal activity.

2.0 END USER'S RESPONSIBILITIES

2.1 HMIS Database Access

End-user will

- Be given limited access to database based upon End-user's job description.
- Read and abide by Maricopa HMIS Agency Partnership Agreement.
- Read and abide by the Maricopa HMIS policy and procedures manual.
- Read, sign, and abide by the HMIS Code of Ethics, which states the End-user has an understanding of the Code of Ethics and agrees to comply with Maricopa HMIS confidentiality practices.

2.2 End-user Identification (I.D.) and Password

End-user will:

- **Not** share End-user identification and password with any person for any reason.
- **Not** transmit End-user identification and password in any form (verbal, written, or electronic).
- Report any suspected mishandling of End-user identification and password.

2.3 Security

End-user will:

- Access the HMIS database only from pre-determined work terminals.

- Log-off the HMIS database and close the Internet browser before leaving a work terminal.
- Log-off the HMIS database and close the Internet browser prior to surfing the Internet.
- Never leave an open HMIS database screen unattended.
- Notify immediately the designated Agency Administrator or the HMIS System Administrator of any suspected security breach.

2.4 Data

2.4.1 Consent Form

End-user will:

- Obtain or confirm the presence of signed client consent form(s) as required by the Provider Agency, state and/or federal laws, and the Maricopa HMIS standards **prior** to entering client information into the HMIS database.
- Be aware of specific protections afforded under Federal Law for persons receiving certain types of services such as domestic violence services, HIV or AIDS treatment, substance abuse services, or mental health services.
- Offer the client the opportunity to input and share additional client information with other Provider Agencies beyond basic identifying data and non-confidential service information.
- Obtain client consent for additional client information and communicate what information will be shared and with whom.

2.4.2 Data Entry

End-user will:

- Only view, obtain, disclose, or use the database information for business purposes related to serving the Provider Agency's clients.
- Enter data into the HMIS database in accordance with the Provider Agency's policies and the Maricopa HMIS minimum data standards.
- Not enter any fictitious or misleading client data.
- Not over-ride or delete information entered by another End-user.
- Edit and/or delete only screens entered by the individual End-user.
- Save data entered at regular intervals. (If the system remains inactive for longer than thirty-minutes, it will automatically log the End-user off the database and not automatically save entered data.)
- Strive for real-time or close to real-time data entry.
- Not enter discriminatory comments made by or about an employee, volunteer, client, or any person based on race, color, religion, national origin, ancestry, handicap, age, sex, and sexual orientation unless direct quotes are deemed essential for assessment, service, and treatment purposes.

- Not enter offensive language and profanity into the HMIS database unless direct client quotes are deemed essential for assessment, service, and treatment purposes.

Agency Administrator will:

- Monitor possible duplication of records, at least every two weeks.
- Delete duplicate client records created by that Agency Administrator's agency users within 24 hours of entry. No duplicate client record may be deleted by any Agency Administrator more than 24 hours after its creation
- Notify the HMIS System Administrator of any duplicate client record(s) identified more than 24 hours after their creation, BY....
- Sending an e-mail to the HMIS System Administrator that includes the duplicate clients' ids', and identifying, if applicable, the client that was created by that Agency Administrator's agency. No client identifying information, i.e. name, SSN, date of birth, etc. will be sent via e-mail.

HMIS System Administrator will:

- Confirm the duplicate client id(s) are only in use by the Provider Agency requesting the deletion. Once confirmed, find out from the Provider Agency which client record is the preferred record and then merge the client records using client merge tool. Once complete, Provider Agency will be notified that the merge is complete so they can remove any duplicative data, if applicable, from the client record..
- If the duplicate client is in use by other Provider Agencies then the System Administrator will determine a) how much data is contained in each client record and b) the date the client was first created in the HMIS database.
 - If the amount of data contained in each client record is unequal, then the System Administrator will notify the Provider Agency or Provider Agencies of the duplicate record(s) and will inform them of the new client id and when the client record merge will take place. Once the record merge is complete, all Provider Agencies will be notified so they can remove any duplicative data, if applicable, from the client record.
 - If duplicate client record(s) contain the same amount of data then the client record with the earliest HMIS creation date will be identified as the correct client record. The System Administrator will then notify the Provider Agency or Provider Agencies using the client record(s) with the later HMIS creation date(s) that their data will be migrated automatically to the client record with the earliest HMIS creation date, when the migration will take place, and they will be given the new client id number(s) for their client(s). Once the record merge is complete, all Provider Agencies will be notified so they can remove any duplicative data, if applicable, from the client record.
 - All client deletions by the System Administrator will be recorded in the HMIS Help Desk software for tracking, audit, and potential future training needs.
- System Administrator will generate quarterly a Client Duplication Report and assist Agency Administrators in correcting duplications, as needed.

2.5 Legal Parameters

End-user will:

- Not transmit any material in violation of United States federal or state law which includes, but is not limited to: copyright material, material legally judged to be threatening or obscene, and material considered protected by trade secret.
- Not use the Maricopa HMIS with intent to defraud the federal, state, or local government or an individual entity, or to conduct any illegal activity.

3.0 MANAGEMENT OF END-USER SERVICEPOINT ACCESS PRIVILEGES

3.1 Administration of End-user Access

3.1.1 Provider Agency Executive Director or designee will:

- Determine End-user's database access level based upon End-user's job description.
- Determine whether End-user needs access to another intra-agency sub-level.
- Authorize Agency Administrator to generate End-user I.D. and password.

3.1.2 Agency Administrator will:

- Enter End-user I.D. and produce computer-generated password within database administration section.
- Assign End-user to another intra-agency sub-level when deemed appropriate.
- Assume responsibility for adding, up-dating, inactivating, and re-activating End-user name and password.

3.2 End-user I.D. format

Agency Administrator will:

- Create an End-user's I.D. using any naming convention. The End-user I.D. should be unique for this system. End-user I.D. is space sensitive and not case sensitive.
- Add a number sequence to the End-user's ID if the original ID has already been used in the system.

3.3 Passwords

3.3.1 Creation:

- The computer automatically generates a temporary password for the new End-user.
- The Agency Administrator communicates this password to the new End-user.

3.3.2 Use:

- End-user must change the password after initially logging correctly into the database.
- The End-user creates a *unique* password between 8 and 16 characters with a minimum of two numbers. The End-user **DOES NOT** use a password used for other purposes; this password must be unique.

- Passwords shall not be, or include, the End-user name, the HMIS name, or the HMIS Vendor's name.
- Passwords should not consist entirely of any word found in the common dictionary or any of the above spelled backwards.
- Password is space and case sensitive.

3.3.3 Expiration:

- Passwords expire every **45 days**.
- End-users must create a new password that is different from the original (expiring) password.

3.4 Termination or Extended Leave from Employment:

3.4.1 Upon Termination, the Agency Administrator will:

- Delete the End-user immediately.
- Assume all responsibility for deleting their End-users from the HMIS system.

3.4.2 Extended Leave from employment:

Agency Administrator will:

- Inactivate an End-user within 5 business days of the beginning of an extended leave period greater than 45 days.
- Activate the End-user upon returning.

4.0 END USER'S ACCESS LEVELS

4.1 Introduction:

Twelve access levels exist in the ServicePoint system. Each level reflects the End-user's access to client-level paper records. Only agency staff and volunteers, who need access to the HMIS database for client data entry, qualify for an End-user license. The level determines the type of information the End-user visualizes.

4.2 End-user level types:

4.2.1 Resource Specialist:

- Access limited **only** to the ResourcePoint module.
 - Views Provider Agency and program information.
 - May search database for other Provider Agencies and programs.
- NO access to client, shelter, or service records.
- Cannot modify or delete data.

4.2.2 Volunteer:

- Access to ResourcePoint.
- Limited access to ClientPoint (client information).

- May view or edit basic demographic information about clients (the profile screen).
- Restricted from all other ClientPoint screens.
- May enter new clients; make referrals, or check-in/out a client from a shelter.
- Limited access to ServicePoint (service records).
 - May view clients' service history.
 - Does not have access to the "Services Provided".

4.2.3 Agency Staff

- Access to ResourcePoint.
- Limited access to ClientPoint.
 - May access basic demographic data on clients (profile screen).
 - Restricted from all other ClientPoint screens.
- Access to most functions in ServicePoint.
 - Full access to service records.
- May add news items to the Newsflash.
- Restricted access to reports.

4.2.4 Case Manager II

- Access to all ClientPoint screens.
- Restricted from administrative functions.
- Access to ServicePoint.
- Full access to reports.
- May add news items to the Newsflash.

4.2.5 Resource Specialist II

- Access limited only to the ResourcePoint module.
 - Views Provider Agency and program information.
 - Search database for other Provider Agencies and programs.
- NO access to client, shelter, or service records.
- Can modify or delete Provider Agency and program information within his/her Provider Agency.
- Cannot modify or delete Provider Agency and program information outside his/her Provider Agency.

4.2.6 Agency Administrator -

- Access to all features, including ClientPoint, ServicePoint, ShelterPoint, ResourcePoint, and NewsFlash.

- Access to Provider Agency level administrative functions.
 - Add/remove End-users for his/her Provider Agency.
 - Edit their Provider Agency and program data.
 - Full reporting access.

4.2.7 Executive Director

- Access to all features, including ClientPoint, ServicePoint, ShelterPoint, ResourcePoint, and NewsFlash. Same access rights as Agency Administrator, but ranked above Agency Administrator (See Glossary).
- Access to Provider Agency level administrative functions.
 - Add/inactivate End-users from his/her Provider Agency including Agency Administrator.
 - Edit their Provider Agency and program data.
 - Full reporting access.

4.2.8 Resource Specialist III

- Access limited only to the ResourcePoint module.
 - View Provider Agency and program information.
 - Search database for other Provider Agencies and programs.
- NO access to client, shelter, or service records.
- Can modify or delete all Provider Agency and program information system wide.
- Access to system-wide news.

4.2.9 System Operator

- No access to ClientPoint, ServicePoint, or ShelterPoint.
- Access to the system-wide administrative functions.
 - Setup new, modify, and delete Provider Agencies/programs.
 - Add new, modify, and activate/inactivate End-users.
 - Reset passwords.
 - Order additional End-user licenses and modify the allocation of licenses.
 - Add, modify, and delete pick-list information.
- Access to system-wide news.

1.3.10 System Administrator I

- Access to ClientPoint, ServicePoint, and ShelterPoint for every Provider Agency.
 - NO access to restricted client data.
- Access to the system-wide administrative functions.
 - Setup new, modify, and delete Provider Agencies/programs.

- Add new, modify, and activate/inactivate End-users.
- Reset passwords.
- Order additional End-user licenses and modify the allocation of licenses.
- Add, modify, and delete pick-list information.
- Access to audit trail for all End-users.
- Access to system-wide news.

1.3.11 System Administrator II

- Access to ClientPoint, ServicePoint, and ShelterPoint for every Provider Agency.
- Access to the system-wide administrative functions.
 - Setup new, modify, and delete Provider Agencies/programs.
 - Add new, modify, and activate/inactivate End-users.
 - Reset passwords.
 - Order additional End-user licenses and modify the allocation of licenses.
 - Add, modify, and delete pick-list information.
- Access to Shadow mode, which allows System Administrator to shadow an End-user and visualize the system through that End-user's access level.
- Access to audit trail for all End-users.
- Access to Dynamic Assessments.
- Access to System-wide news.

USER TYPES AND ACCESS LEVELS

	Resource Specialist I	Resource Specialist II	Resource Specialist III	Volunteer	Agency Staff	Case Manager I & II	Agency Administrator	Executive Director	System Operator	System Administrator I	System Administrator II
<i>ClientPoint</i>											
Profile				X	X	X	X	X		X	X
Assessments						X	X	X		X	X
Case Notes						X	X	X		X	X
Case Plans						X	X	X		X	X
Service Records				X	X	X	X	X		X	X
<i>ServicePoint</i>											
Referrals				X	X	X	X	X		X	X
Services Provided					X	X	X	X		X	X
<i>ResourcePoint</i>	X	X	X	X	X	X	X	X	X	X	X
<i>ShelterPoint</i>				X	X	X	X	X		X	X
<i>Reports</i>											
<i>Audit Reports</i>											
<i>Client/Service Information</i>							X	X		X	X
<i>User Information</i>			X				X	X		X	X
<i>Client/Service Access Information</i>											X
<i>Provider Reports</i>											
<i>Client Served</i>						X	X	X		X	X
<i>Daily Bed Report</i>			X			X	X	X		X	X
<i>Entry/Exit Report</i>						X	X	X		X	X
<i>Exhibit 1 Report</i>											X
<i>HUD 40118 APR</i>						X	X	X		X	X
<i>PATH Report</i>						X	X	X		X	X
<i>Outstanding Maricopa Homeless Management Information System Referrals</i>						X	X	X		X	
<i>Maricopa HMIS Web Site</i>											
<i>Service Transaction</i>						X	X	X		X	X
<i>Needs Report</i>						X	X	X		X	X

Local Data Storage

- Policy:** The Provider Agency assumes responsibility for client records containing identifying information stored within the Provider Agency's local computers.
- Purpose:** To outline the Provider Agency's responsibility for client-identified data.
- Scope:** Provider Agencies
- Definitions:**
- Client:* Any person, who received, applied for or was denied services by a Provider Agency.
- Client-identifying Information:* Any information that would allow an individual client to be identified including but not limited to name, nick name, social security number, military ID number or medical insurance ID number.
- End-user:* Any person given access to the database including staff and volunteers.
- Maricopa HMIS database:* The Homeless Management Information System's database, also known as HMIS database and/or database.
- Provider Agency:* An agency authorized to participate in the Maricopa County Homeless Management Information System.

Procedure:

1.0 RESPONSIBILITIES

1.1 Provider Agency

- Assumes the responsibility for client-identifiable information stored at the agency including computer data storage, paper copies and reports downloaded from the HMIS database.
- Develops, implements, and maintains written policies for the management, protection, and transmission of client-identifying information stored on local agency computers, agency files, and reports.
- Assures policies remain consistent (regarding client-identifying information) with the information security policies outlined in the Maricopa HMIS Policy and Procedure Manual.

1.2 Maricopa HMIS

- Assumes **no** responsibility for the management, protection, and transmission of client-identifying information stored on local agency computers, agency files, and reports.

Virus Control Management

Policy: Maricopa HMIS workstations and servers maintain state-of-the-art malicious code and malicious intrusion protection.

Purpose: To educate Provider Agencies on malicious code types and effective methodology for avoiding infection.

Scope: System wide computers

Definitions: *Computer virus:* A self-replicating piece of computer code, which resides in active memory and partially or fully attaches itself to files and/or applications. (See types of viruses at the Appendix of this document.)

Computer Worm: Similar to viruses, worms reside in active memory of computers and replicate themselves and will usually interfere with normal computer use or a computer program. Unlike viruses, worms exist as separate entities and do not attach themselves to other files or programs.

Firewall: A system or group of systems that enforce an access control policy between two networks. The system may contain a pair of mechanisms: one that exists to block Internet traffic, and the other that exists to permit Internet traffic.

Malicious code: An illegitimate computer code, which produces an undesired effect including Trojan horses, viruses and worms.

Self-replicate: Make copies of itself.

Trojan horse: A malicious, security-breaking program, which pretends to be a benign application such as a screen saver, a game, or some other valuable program; but purposefully causes something the user does not expect. Unlike a virus, Trojan horse do not replicate, but Trojan horse programs attacks pose one of the most serious threats to computer security.

Responsibilities: HMIS System Administrator and HMIS Provider Agencies.

Procedure:

1.0 INTRODUCTION

Malicious codes, delivered through various means, are designed to delete, scramble End-user files/ programs and/or disable specific computer functions. At times a malicious code slows down a computer--- a mere inconvenience; other times a malicious code causes an entire system shut down. With over 24,000 known malicious codes circulating in the world today, and more being

discovered every day, the Provider Agency must learn how to protect its computer system. Since the computer industry progresses at a rapid rate, each Provider Agency must keep current on protective procedures by consulting with computer system experts periodically for the latest in malicious code preventative measures.

2.0 VIRUS PROTECTION

- 2.1 Maricopa HMIS Provider Agencies shall purchase and maintain state-of-the art, commercially produced virus protection software, which includes automated scanning of files.
- 2.2 Bowman Internet Systems shall maintain state-of-the art, commercially produced virus protection software for the Maricopa HMIS server(s).

3.0 FIREWALLS

- 3.1 Maricopa HMIS workstations shall maintain secure firewalls to protect against malicious intrusions. The firewall must be a part of a consistent overall Provider Agency security architecture.
- 3.2 Bowman Internet Systems shall maintain secure firewalls for the Maricopa HMIS servers.

Monitoring Provider Agency Compliance

Policy: CI&R and the Maricopa Homeless Management Information System (HMIS) staff monitor and review the Provider Agencies' adherence to HMIS security, confidentiality regulations and quality standards.

Purpose: To ensure the Provider Agencies abide by HMIS security, confidentiality regulations and quality standards.

To provide a specific course of action for HMIS Policy and Procedure violations.

Scope: System wide

References: Maintenance of Client Confidentiality Policy and Procedure

Definitions: *Consultation:* A discussion, usually by phone, reminding the End-user or Provider Agency, of proper security and/or confidentiality practice(s), following confirmed inappropriate action(s).

HMIS Provider Database: A software application, which allows HMIS staff to track all communication relating to Provider Agencies.

Probation: A trial period of time, not greater than one hundred and eighty days (180), in which an End-user or Provider Agency addresses and corrects inappropriate action(s).

Quality of Data Issue – Any concern that decreases the accuracy and completeness of the data as defined by the Minimum Data Requirement.

Reinstatement Corrective Action Plan - A modified Corrective Action Plan developed specifically for the purpose of preparing and assessing the appropriateness of reinstating a previously terminated Agency as an HMIS Provider Agency.

Sanctions: Penalties for noncompliance specified by the HMIS User Group and the CI&R Executive Director.

Suspension: An act of postponing database access, after an End-user or Provider Agency receives written notice via certified mail explaining a breach of contract, quality of data issue or improper security and/or confidentiality practices, where the guilty party received previous warning(s) and did not correct inappropriate actions.

Termination: The act of ending database access, after an End-user or Provider Agency receives an appropriate written notice via certified mail explaining the reasons for cessation of database use.

Written Warning: A printed notice informing the End-user or Provider Agency of a confirmed inappropriate action and a corrective explanation of the desired conduct.

Procedure:

1.0 MONITORING PROVIDER AGENCY AND END-USER'S ACTIONS

1.1 The HMIS System Administrator (SA):

- Receives quality assurance reports from the HMIS technical support staff.
- Reviews compliance with identified issues outlined in the corrective action plans. (See Corrective Action Plan Policy for further details)
- Coordinates with HMIS technical support staff, who monitor the corrective actions for non-compliance issues and/or inappropriate actions.
- Checks Provider Agency's file and HMIS Provider Database for previous compliance actions or sanctions.
- Determines the appropriate action (see 1.3) and directs the course of action based upon previous compliance responses, actions and sanctions.
- Reports resolution of corrective actions to User Group and CI&R Executive Director.

1.2 HMIS Technical Support Staff:

- Monitors the corrective actions for non-compliance issues and/or inappropriate actions as directed by the HMIS SA.
- Enters the violation, corrective action plan, correspondence summaries and performance improvement items into the Provider Agency's Profile through a managed database.
- Maintains copies of correspondence and/or reports in the Provider Agency's file.
- Assists Provider Agencies when deemed necessary.

1.3 HMIS User Group:

- Assists the HMIS SA and CI&R Executive Director in determining appropriate action for non-emergency HMIS violations. (See 3.1.1 for emergency intervention)
- Reviews and updates the Corrective Action Plan Policy annually.

2.0 HMIS PROVIDER DATABASE

2.1 The HMIS staff enters data into the HMIS Provider Database to produce reports on tracked areas. At a minimum, the reports include:

- Provider Agency (or End-user) Policy and Procedure violation report.
- Appeals and Grievance Report
- Complaint Report
- Incident Report

- Data Quality Report
- Minimum Data Quality Report
- Corrective Action Plan Compliance Report
- Correspondence Report
- Performance Improvement Report

2.2 The HMIS staff produces the above reports by request from the HMIS SA, CI&R Executive Director or the HMIS User Group.

3.0 SEQUENCE OF PROCEDURES

3.1 Introduction: After a confirmed report of a HMIS procedural violation, the HMIS SA Administrator implements action within 24 hours.

3.1.1 In emergency situations i.e. security breach and/or emanate danger to the database, the HMIS System Administrator immediately contacts and reports to the CI&R Executive Director, who has final authority for the impending action.

3.1.2 In all other cases, the HMIS SA implements a course of action outlined in the following steps:

- Step 1: Consultation with the Provider Agency
- Step 2: Written warning
- Step 3: Sanctions
- Step 4: Probation
- Step 5: Suspension
- Step 6: Termination

3.2 Step 1: Consultation with the Provider Agency

The HMIS SA:

- Contacts and discusses the inappropriate practice with the Provider Agency Administrator.
- Itemizes specific requirements for improvement.
- Identifies a time frame for implementation and completion of the corrective measure(s).
- Coordinates further training if deemed necessary.
- Documents conversation and reports this information to technical support staff for database entry.
- Alerts technical support staff to begin monitoring procedures, which remain in place until resolution.

3.3 Step 2: Written Warning

- 3.3.1 If the corrective measure(s) never comes to fruition or if the inappropriate practice(s) continues over an extended period of time (3 months) or greater, the HMIS SA, under the guidance of the HMIS User Group and CI&R Executive Director, implements a written warning procedure.
- 3.3.2 The HMIS SA or an appropriate HMIS staff member (under the HMIS SA instruction) sends a written notice, via certified mail, to the Provider Agency Administrator which includes:
- An explanation of violations and itemizes specific requirements for improvement as defined through a Corrective Action Plan. (See Corrective Action Plan Policy)
 - A time frame for implementation and completion of the corrective measure(s).
 - A copy of the written summary documenting the HMIS System Administrators, User Group and CI&R Executive Directors review of the Provider Agency's profile.
 - A training or technical assistance plan, if deemed necessary.
 - Further HMIS actions if the inappropriate practice(s) continue.
- 3.3.3 The technical support staff archives a copy of the written warning in the Provider Agency's file, the Provider Agency receives the original written notice.
- 3.4 Step 3: Sanctions
- 3.4.1 If the Provider Agency fails to provide satisfactory responses to the written warning within the allotted time period, as defined in the Corrective Action Plan, then the HMIS SA presents the updated Provider Agency file to the HMIS User Group and CI&R Executive Director.
- 3.4.2 The HMIS User Group and CI&R Executive Director review all previous correspondences and/or Provider Agency corrective action responses and determine sanctions based on the evidence.
- 3.4.3 The HMIS SA notifies via certified mail the Provider Agency of impending sanctions, the effective date, a copy of the original written notice, a copy of the HMIS Grievance Policy and this policy.
- 3.4.4 The technical support staff archives a copy of the sanctions notification in the Provider Agency's file, the Provider Agency receives the original written notice.
- 3.5 Step 4: Probation
- 3.5.1 If the Provider Agency fails to provide satisfactory responses to the sanctions within the allotted time period, then the HMIS SA presents the updated Provider Agency file to the HMIS User Group and CI&R Executive Director.
- 3.5.2 The HMIS User Group and the CI&R Executive Director review all previous correspondence and Provider Agency corrective action responses and determine warranted probation.
- 3.5.3 The HMIS System Administrator
- Notifies via certified mail the Provider Agency of impending probation and the effective date.

- Assigns Technical Support staff to work with and monitor resolution of identified areas of violation.

3.5.4 The notification:

- Explains the violation(s) and itemizes specific requirements for improvement.
- Identifies assigned HMIS staff, who will work collectively with the Agency Administrator and Executive Director, to determine the reason(s) for ineffective corrective measures and create a time-line for effective resolution.
 - Includes a copy of the HMIS User Group's and the CI&R Executive Director's review of the Provider Agency's issues.
 - Explains the change in provider status to Probationary Provider Agency.

3.5.5 The probationary period remains effective until all corrective measures meet the HMIS User Group's and CI&R Executive Director's approval and will not persist past one hundred and eighty (180) days from the notification date.

3.5.6 The technical support staff archives a copy of the probation notification in the Provider Agency's file; the Provider Agency receives the original written notice.

3.6 Step 5: Suspension

3.6.1 If the Probationary Provider Agency's inappropriate practice(s) continues or reoccurs, and there is no resolution with the HMIS System Administrator and HMIS staff satisfactory to the HMIS User Group and CI&R Executive Director, then the HMIS System Administrator begins the suspension process.

3.6.2 The HMIS System Administrator:

- Notifies via certified mail the Provider Agency of impending suspension and the effective date.
- Assigns appropriate HMIS staff to facilitate data identification and data transfer to another database.
- Immediately inactivates all Provider Agency End-user database access.
- Only reactivates End-user access after receiving written permission via e-mail or fax from the HMIS User Group and/or the CI&R Executive Director.

3.6.3 The notification:

- Identifies assigned HMIS staff, who will work collectively with the Provider Agency Administrator and Executive Director, to identify and transfer database elements needed for the Provider Agency to continue conducting business.
- Includes an updated copy of the HMIS User Group's and the CI&R Executive Director's review and decision to suspend Provider Agency's HMIS access.
- Explains the change in provider status to Suspended Provider Agency and the suspension of all End-user database access.
- Explains the requirement of a mandatory meeting to address the resolution of inappropriate practices. The HMIS SA coordinates the meeting time and place with all

participants, which include the Agency Administrator and/or the Executive Director, HMIS User Group representatives and the CI&R Executive Director.

- Explains the possibility of the Provider Agency losing HUD funding.

3.6.4 The technical support staff archives a copy of the suspension notification in the Provider Agency's file; the Provider Agency receives the original written notice.

3.7 Step 6: Termination

3.7.1 If the Probationary Provider Agency refuses to attend the mandatory meeting or comply with HMIS Policy and Procedures, then the CI&R Executive Director issues an order to the HMIS SA to permanently terminate the Provider Agency access to the HMIS database.

3.7.2 HMIS SA notifies via certified mail the Provider Agency the effective date of termination.

3.7.3 Data Transfer

3.7.3.1 The Terminated Provider Agency

- Must submit a request for their data within 60 days of termination.
- Assumes responsibility for cost of data transfer to another database.
- Pays the HMIS accountant prior to data delivery.

3.7.3.2 The CI&R Executive Director, in conjunction with Bowman Internet Systems, provides a detailed cost analysis and time-line of data transfer.

3.7.4 The CI&R through Bowman Internet Systems will provide the data file in ASCII delimited format only.

4.0 REINSTATEMENT

4.1 The Terminated Provider Agency may request reinstatement once previous violations have been addressed and corrected.

4.2 Reinstatement Process:

Responsible Party	Action
Terminated Provider Agency	<ul style="list-style-type: none"> • Contacts CI&R Executive Director. • Fills out Reinstatement Corrective Action Plan*, which identifies violation(s) and concerns. • Provides documented evidence of corrective procedures. • Establishes a time-line for completed corrective procedures.
CI&R Executive Director	<ul style="list-style-type: none"> • Acknowledges within 24 hours receipt of the Reinstatement Corrective Action Plan via e-mail or phone. • Reviews and determines feasibility of Reinstatement Corrective Action Plan. • Contacts Provider Agency, within three working days, with any modifications to or approval of the submitted Reinstatement Corrective Action Plan. • Assesses corrective process and time-line adherence.

	<ul style="list-style-type: none"> • Makes recommendations to HMIS User Group.
HMIS User Group	<ul style="list-style-type: none"> • Reviews Reinstatement Corrective Action Plan. • Accepts or denies reinstatement. • Contacts the Provider Agency when Reinstatement Corrective Action Plan meets satisfactory completion or if further action will be taken. • Reports the decision to CI&R Executive Director.
CI&R Executive Director	<ul style="list-style-type: none"> • Contacts Provider Agency with HMIS User Group decision and recommendations. • Instructs HMIS System Administrator to re-activate the Agency Administrator/Executive Director User License when applicable.
HMIS System Administrator (SA)	<ul style="list-style-type: none"> • Reactivates Agency Administrator/Executive Director User License. • Reports to the HMIS User Group and CI&R Executive Director of reinstatement date. • Re-activates Probationary Status. • Instructs HMIS staff to begin coordinating time-line dates and corrective changes into the monitoring procedure.
HMIS Staff	<ul style="list-style-type: none"> • Monitors the Reinstatement Corrective Action Plan. • Reports outcomes on a weekly basis to the HMIS SA. • Contacts HMIS System Administrator immediately of any further breaches of Policies and Procedures. • Files completed report in Provider Agency file.

Corrective Action Plan

Policy: The Maricopa Homeless Management Information System (HMIS) User Group develops, implements and maintains methods for correcting inappropriate database use.

Purpose: To establish guidelines and procedures to aid the HMIS System Administrator and HMIS staff in assisting Provider Agency's compliance with HMIS Policy and Procedures.

Scope: All Maricopa HMIS Staff and HMIS User Group

References: Maintenance of Client Confidentiality
Monitoring Provider Agency Compliance

Procedure:

1.0 HMIS VIOLATIONS

1.1 Access and use of the HMIS database by HMIS Provider Agency staff and HMIS support staff is limited to the performance of their authorized job function. All other types of use are strictly forbidden and considered a Code of Ethics, Maricopa HMIS Policy and Procedures and/or the Agency Partnership Agreement security violation.

1.2 The HMIS System Administrator and/or the User Group may be contacted for clarification and guidance on possible HMIS violations.

2.0 PROVIDER AGENCY CORRECTIVE ACTION PLAN

2.1 When an Agency Administrator becomes aware of a security violation within their agency, they will report the violation to the System Administrator immediately and provide the appropriate corrective action plan documentation.

2.2 In the event of confirmed HMIS violation(s) by the Provider Agency or it's End-user(s), the HMIS System Administrator or appropriate HMIS staff member contacts the Provider Agency Executive Director or Agency Administrator and begins the Corrective Action Plan process

2.2 Corrective Action Plan Process:

Responsible Party	Action
HMIS System Administrator (SA)	<ol style="list-style-type: none">1. Contacts Provider Agency.2. Identifies violation(s).3. Provides references to the applicable HMIS Policy and Procedure.4. Instructs Agency Administrator-Executive Director on how to fill out the Corrective Action Plan.5. Identifies any HMIS training or resources that may assist in correcting issues.

	6. Assists in coordinating a reasonable time-line.
Agency Administrator	<ol style="list-style-type: none"> 1. Fills out Corrective Action Plan. 2. Submits Corrective Action Plan within one week of notification via e-mail or certified mail to HMIS System Administrator. 3. Contacts via phone and notifies the HMIS System Administrator.
HMIS System Administrator	<ol style="list-style-type: none"> 2. Acknowledges within 24 hours receipt of the Corrective Action Plan via e-mail or phone. 3. Reviews and determines feasibility of submitted Corrective Action Plan. 4. Contacts Provider Agency, within three working days, with any modifications to or approval of the submitted Corrective Action Plan. 5. Instructs HMIS staff to begin coordinating time-line dates and corrective changes into the monitoring procedure.
HMIS Staff	<ol style="list-style-type: none"> 1. Monitors the Corrective Action Plan. 2. Reports outcomes for each step in the Corrective Action Plan, on a weekly basis to the HMIS System Administrator. 3. Contacts immediately HMIS SA of any further breaches of Policies and Procedures.
HMIS System Administrator	<ol style="list-style-type: none"> 1. Assesses corrective process and time-line adherence. 2. Reports to the HMIS User Group and CI&R Executive Director areas of non-compliance. 3. Contacts the Provider Agency when Corrective Action Plan meets satisfactory completion or if further action will be taken (See Provider Agency Monitoring and Compliance Policy).
HMIS Staff	<ol style="list-style-type: none"> 1. Files completed report in Provider Agency file.

2.4 The Corrective Action Plan (see attachment) includes the following:

- Date of Notification
- Name of Provider Agency and End-user(s), when applicable
- Itemized specific violations
- A time frame for corrective measure(s) implementation and completion
- Itemized steps for corrective measures
- HMIS resources to be allocated: training, equipment, documents
- HMIS staff contact names, telephone numbers and e-mail addresses
- HMIS System Administrator physical and E-mail address

3.0 RESPONSIBILITIES

3.1 HMIS System Administrator and HMIS Staff:

- Monitor the corrective actions process for non-compliance issues and/or inappropriate actions.
- Identify further opportunities for improvement.
- Identify potential best practices.
- Assist in allocating HMIS resources and developing solutions for non-compliance issues, when possible.

- Maintain copies of correspondences and/or reports in the Provider Agency's file.
- 3.2 HMIS User Group:
- Reviews and updates Corrective Action Plan Policy annually.
 - Instructs HMIS System Administrator and HMIS Staff on development and implementation of additional monitoring reports and methodologies for identifying inappropriate actions.

Maricopa HMIS Corrective Action Plan

Date of Notification: _____

Name of Provider Agency: _____

End-user(s) (when applicable) _____

Itemized violations

Applicable Document**

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____

Itemized Corrective Measures

Expected Completion Date

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____

HMIS Resources

Contact HMIS Staff Name and Number

1. _____
2. _____
3. _____
4. _____
5. _____

First Last Name
Agency Administrator/Executive Director

Signature

** (Code of Ethics, Agency Partnership Agreement, HMIS Policy & Procedure)

Send to the following address:

HMISsupport@cox.net OR mail to: HMIS System Administrator,
Community Information & Referral, Inc.
1515 E. Osborn Road
Phoenix, AZ 85014

P&P#: II - 06
Approved by: HMIS User Group

Effective Date: _____
Last Revision Date: _____

Risk Assessment and Disaster Recovery – Pending

Data Quality Assurance

Policy: The Maricopa HMIS Project will maintain an on-going process of Quality improvement. This process will be built around routine End-user meetings that occur at multiple levels of the implementation and routine measurement of data quality and outcomes related to mission critical processes.

Purpose: To insure data is accurate and to identify and problem solve barriers.

Scope: All Maricopa HMIS Staff and HMIS User Group

Procedure:

1.0 User Meetings

1.1 Purposes:

- Opportunity for Benchmarking between participants
- Review core processes and related measures:
 - Identify issues and share solutions
 - Identify those issues where additional help is needed
 - Incorporate process and outcome measures. (For example Maricopa HMIS Project requires coverage rates types of reports generated at the Provider Agency level)
- Support transparency
- Share successes
- Review aggregated data
- Formalize communication between Provider Agency and System Administrators
- Provides routine End-user satisfaction input

1.2 Types and Frequencies

- Agency Administrator / User Group Meetings – bi-monthly
- Data Quality sub-committee meetings – bi-monthly
- Specialty Provider Agency Meetings (as needed):
 - Domestic Violence
 - Runaway Youth
 - Housing Specialists
 - Mental Health
 - Homeless Education Providers

1.3 Meeting Requirements

- Minimum attendance levels (= all those with End-user licenses + leadership)
- Structured Meeting Agenda reviewing core processes:
 - Coverage – Are all the clients being entered? What % of the homeless are in the System?
 - Client Refusals

- Data Quality – null data fields, # of data corrections
- Interview issues
- Definition questions
- Training needs
- Privacy and Security issues
- Reports: Review Provider Agency aggregated data
- Structured Minutes with copy sent to System Administrator to monitor End-user meeting compliance with the Maricopa HMIS Project contract

1.4 Additional Processes related to System Administrator and Maricopa HMIS Project Meetings

- System Access / Licenses
- System Performance
- Routine Support / Help Desk
- Contract Compliance (Provider Agency and Vendor)

2.0 Sources of Data

- End-user input from structured minutes
- Qualitative and Quantitative
- Measures that result from routine queries within the database
- Short Term measures to assess problem resolution
- End-user Satisfaction Surveys

3.0 Improvement Cycle

- Assess variation /one time variation due to unique conditions or sustained issue
- Prioritize problem solving
- Define a plan for change
- Test the success of your changes

4.0 Measurement Grid

Process	Measure (control chart / sentinel event)
Coverage	<ul style="list-style-type: none"> ● Provider Agency -% of planned entry completed -monthly ● CoC-% of housing chart covered – annual
Training	<ul style="list-style-type: none"> ● # of End-users trained ● Follow-up Satisfaction Surveys (Minutes) ● # of records identified in data integrity reports
Privacy	<ul style="list-style-type: none"> ● Grievances or breaches ● Privacy Issues identified on Minutes ● % of clients entered as unnamed aka anonymous ● % of Provider Agencies with profile closed
Performance	<ul style="list-style-type: none"> ● Average System response time on “saves” and “report generation” sampling weekly at different times

- # of System bugs reported to Vendor
- Help Desk
- % of help desk inquiries answered during call, within 1 day, within 3 days & within 1 week
 - % of unresolved or follow-up Help Desk requests
 - End-User Satisfaction – minutes
- Access
- Audit of Provider Agency training log forms against End-users in the System
 - # of license/End-user variations

5.0 Data Quality

5.1 Data must pass “Fitness for Use” Tests

- Completeness
 - Information is entered on all clients
 - Information on the client is complete
- Accuracy
 - Data reflects reality
 - Data is entered correctly
 - Data has face validity – reflects what we know
- Consistency
 - Performance information is consistent across time

6.0 Common Errors

- Systematic Errors/ Issues with Training
 - Entering “no” when you mean “yes”
 - Definition drift
 - Entering text without using drop down
 - Entering text without using drop down
- Random Errors/Sloppy Entry/Workflow
 - Date Errors (DOB is 4/15/52, entered 4/15/04)
 - Transposing numbers
 - Spelling errors (Lauren vs. Loren)
 - Accidentally selecting the wrong response from a drop down

7.0 Factors impacting quality

- Prioritized Process in the Organization?
 - Are End-users given the time to participate in training and to complete entry?
 - Is the environment arranged to support entry?
 - Is the process owner within the Provider Agency respected?
 - Is the data used?

8.0 Provider Agency Procedures for ensuring Quality

- Standardized collection instruments

- Creating an environment conducive to data collection and entry
- Event triggers for data collection and entry – clearly defined work flow
- Guidance for special populations
- Must run reports monthly!

9.0 Maricopa HMIS Project Procedures for ensuring quality

- HMIS staff monthly reviews reports for completeness, accuracy, and consistency
- Clear protocols for correcting data
 - Provider Agency signs off on reports monthly
 - Errors systematically result in corrective action
 - Procedures for correcting are defined
- Software has error checking functions (out of range, missing values, incongruous data)
- Provider Agency Staff looks at data reliability and validity issues prior to publishing reports. Collecting Provider Agencies will know which questions result in data that simply is not stable. Do the findings make sense? Must be knowledgeable about local services to recognize systematic data errors.
- Using the data

10.0 Measures to Monitor Quality

- Queries
 - Null DOB and gender fields
 - Rate of infants under the age of 1
 - Gender by family relationship
 - Homeless by “extent of homelessness”
 - HUD Assessment by entries & exits
 - Age by family relationship
 - Number of End-users and records on the live site
 - Null exit dates related to short term services
 - Ambiguous data in reports

11.0 Available ART Reports for Monitoring Data Quality

- Active Clients Not Assigned to a Program: This is a list of clients that have a level 1 (agency) entry/exit instead of a level 2 or 3 (program/grant) entry/exit. This report is only for Entry/Exits as ShelterPoint tracks the program when a client is placed in a bed.
- Active Clients Without an Exit Date: This is a list of clients that don’t have an exit date. This is for comparing this list to the client list agencies keep on paper to make sure everything is in synch.
- Age Requirement: This is a list of clients that don’t fit within a specified age range. For example, if an agency only accepts youth then they could run the report for 0 to 17 and find any clients that are outside their program requirements.
- Blank Date of Birth: This is a list of clients that do not have a date of birth. This data element is required for all clients according to the HUD Data Standards.

- Blank Unemployed for Adults: This is a list of adult (over 17) clients that didn't answer the unemployed/employed question. This data element is required for all adults according to the HUD Data Standards. It is also required for all unaccompanied youth.
- Chronically Homeless Households: This is a list of clients in households that have answered the question "Is the client chronically homeless" yes. According to HUD, a chronically homeless client can only be single.
- Chronically Homeless Without a Disability: This is a list of chronically homeless clients that didn't answer the "Does the client have a disability of long duration" or left it blank. According to HUD, a chronically homeless client must have a disability of long duration.
- Client Gender not Matching Program: This is a list of clients whose gender doesn't match the program requirements. This is useful for mainly single adult shelter or family shelters that don't allow adult males.
- Clients not Homeless or Unanswered: This is a list of clients who either didn't answer the question "Is the client homeless?" or answered the question No.
- Clients with Chronic not Matching Extent of Homelessness: This is a list of clients that are marked chronically homeless but don't have an extent that matches that answer. For example, a client that is first time homeless or has 1-3 episodes of homelessness doesn't meet the definition of chronically homeless.
- Domestic Violence Victims with no Extent Listed: This is a list of domestic violence victims that didn't answer the extent of domestic violence question. The extent of domestic violence question is required for all clients that answered yes to the domestic violence victim question.
- Employed with Nulls: This is a list of adult (over 17) clients that are employed and didn't answer the Hours Worked Last Week and/or Select Tenure questions. These data elements are required for all adults according to the HUD Data Standards. It is also required for all unaccompanied youth.
- Extent of Homelessness = HOME Program: We have a program that is funded by HOME instead of HUD and they don't require the client to be homeless. So we added a picklist option to this data element and a few others for that program only. This query is for those that aren't a HOME program to check and make sure their staff didn't choose this picklist option.
- Females with Pregnant Question not Answered: This is a list of female clients of child-bearing age (≥ 14) that didn't answer the pregnant question. This question is required for all female clients of child-bearing age according to the HUD Data Standards.
- Future Entry/Exit Dates: ServicePoint allows users to put in future entry/exit dates into ServicePoint. This report allows agencies to clean up those entry/exits.

- Future ShelterPoint Start/End Dates: ServicePoint allows users to put in future start/end dates into ShelterPoint. This report allows agencies to clean up those entries.
- Homelessness Primary Reason HOME Program: We have a program that is funded by HOME instead of HUD and they don't require the client to be homeless. So we added a picklist option to this data element and a few others for that program only. This query is for those that aren't a HOME program to check and make sure their staff didn't choose this picklist option.
- Homelessness Primary Reason not Matching DV Victim: This is a list of clients that listed their homelessness primary reason as domestic violence but answered the domestic violence victim question no or left it blank.
- Household of 1: This is a list of clients that are in a household by themselves. According to HUD a household must contain at least one adult (over 17) and one child (under 18) in order to be considered a household.
- Households with no Head of Household: This is a list of households in which no one is marked as the head of household. This answer is necessary for a bunch of reports.
- Households with More than 1 Head of Household: This is a list of households in which there is more than one head of household. A household can only contain one head of household according to the data standards.
- No Financial Resources and Income: This is a list of clients that have a source of income of no financial resources but the source amount is greater than 0.
- Not a Domestic Violence Victim but have Extent Listed: This is a list of clients that answered no to the domestic violence victim question but completed the extent of domestic violence question.
- Pregnant but no Due Date: This is a list of pregnant females that didn't answer the due date question. This question is required for all pregnant females according to the HUD Data Standards.
- Pregnant Males: This is a list of male clients that answered the pregnant question yes.
- Primary Race and Secondary Race Same: This is a list of clients that have the same primary race and secondary race. According to HUD, this is invalid. It can also cause errors on some reports, including the AHAR.
- School-aged children in School with Missing Answers: This is a list of school-aged (5-17) children in school that didn't answer the school name and/or type of school questions.
- School-aged children not in School with Missing Answers: This is a list of school-aged (5-17) children not in school that didn't answer last date of enrollment and/or didn't list enrollment difficulties.

- School-aged children with in School question Left Blank: This is a list of school-aged (5-17) children that didn't answer the currently in school question.
- SSDI Income and no Disability: This is a list of clients that are receiving disability income but don't have a disability listed.
- SSN Data Quality: This is a four-part report that lists various data input issues related to the SSN data Quality field.
- Unemployed with Null Looking for Work: This is a list of adult (over 17) clients that are unemployed and didn't answer the looking for work question. This data element is required for all adults according to the HUD Data Standards. It is also required for all unaccompanied youth.
- Veterans with no Additional Information: This is a list of adult (over 17) clients that are veterans but didn't answer one or more of the many questions related to veterans.
- Veterans Pension vs. Veterans Status: This is a list of adult (over 17) clients that are receiving a veteran's pension but answered the veteran question no or left it blank.
- Veterans under 18: This is a list of clients under 18 that answered the veteran question yes.
- Zip Code and Zip Code Data Quality: This is a two part report. The first part is a list of clients that have a zip code but have don't know or refused listed for the zip code data quality. The second part is a list of clients that don't have a zip code but have full zip code reported as the data quality code.

III – PRIVACY AND CONFIDENTIALITY

Maintenance of Client Confidentiality

Policy: The Provider Agency adheres to relevant federal, state and local confidentiality regulations and laws that protect client records and only releases confidential client records with written consent by the client, or the client's guardian, unless otherwise provided for in Federal, state or local regulations or laws.

Purpose: To provide guidelines for ensuring maintenance of client confidentiality.

Scope: All Homeless Management Information System (HMIS) Provider Agencies, HMIS End-users and their clients.

Definitions: *Anonymous client:* A client entered into the database with a unique computer generated identifying code acting as a reference for that client.

Client: Any person who received, applied for or was denied services by a Provider Agency.

Client's guardian: Any person legally responsible for a minor or an adult, according to Arizona Revised Statutes (A.R.S.). All references to "client" in this policy also apply to "client's guardian."

End-user: Any person given access to the database including staff and volunteers.

Maricopa HMIS database: The Homeless Management Information System's database, also known as HMIS database and/ or database.

Provider Agency: An agency authorized to participate in the HMIS.

Restricted client: A client whose name is known by only the entering Provider Agency, HMIS System Administrator II, and those agencies the client grants access to his/her name.

Procedure:

1.0 PROVIDER AGENCY'S RESPONSIBILITIES

1.1 Laws and Regulations:

A Provider Agency will abide by:

- All Federal Confidentiality Regulations including those contained in the Code of Federal Regulations, 42 CFR Part 2 (regarding disclosure of alcohol and/or drug abuse records).
- Health Insurance Portability and Accountability Act of 1996 (HIPPA) when applicable.
- Arizona state laws and Federal laws related to confidentiality and security of medical, mental health and substance abuse information including Arizona Revised Statutes Title 12, Arizona Revised Statutes Title 36, 42 CFR Part 2 and all other relevant statutes, rules and regulations.

1.2 Client Consent

A Provider Agency will:

- Provide verbal explanation of Maricopa HMIS and arrange for, when possible, a qualified interpreter or translator for a client not literate in English or having difficulty understanding the consent form(s).
- Be prepared to explain (to the client) security measures used to maintain confidentiality.
- Explain the client's right to be entered as an anonymous client or as a restricted client, if client denies authorization to share basic identifying information or non-confidential service data.
- Obtain from the client a current, signed Client Acknowledgement of Data Entry into the Maricopa Homeless Management Information System form, when applicable to Provider Agency's policy and procedures.
- Prior to release of any client information beyond the basic client profile, obtain from the client a signed release of information form that meets the Provider Agency's standard release of medical, financial and/or any other information regarding the client.
- Place all client authorization forms in an on-site filing system for periodic CI&R audits.
- Retain all client authorization forms for a five-year period upon expiration.
- Retain sovereignty in regards to denying a client service based upon client's willingness to be entered and shared into the HMIS database.
- Insure that all Provider Agency End-users will comply with the requirements for informed consent and client confidentiality.

1.3 Client Information/Data

A Provider Agency will:

- Enter client information into the database only AFTER obtaining a current, signed client consent, if deemed appropriate by the agency's policy and procedures.
- Share client information in the database to other HMIS Provider Agencies only AFTER obtaining a current, signed client consent to share information, if deemed appropriate by the Provider Agency's policy and procedures.
- Not solicit or input client information into the database unless the information proves essential in providing services, developing reports and providing data, and/or conducting evaluations and research.
- Not divulge any confidential information received from the client or the HMIS database to any organization or individual without a current client release form, unless otherwise permitted by relevant regulations or laws.
- Enter in the minimum data required by the HMIS. Any or all client data including client identifiable and confidential information may be restricted to other Provider Agencies.

2.0 PROVIDER AGENCY'S CLIENT RIGHTS

2.1 A client has the right to:

- Decline entrance into the HMIS database. However, the Provider agency determines whether or not to provide services to the client.
- Authorize sharing of personal information to other HMIS Provider Agencies.
- Determine what type of information will be shared and with whom (other HMIS Provider Agencies).
- Request entrance into the database as an anonymous client or a restricted client.
- Rescind acknowledgement and consent for the entry of future information and further participation by completing and sending the Rescinding Client Consent form to the HMIS System Administrator, either through a Provider Agency or registered mail. However, data already within the database will remain accessible to the Provider Agencies who have entered data on that particular client according to Federal and State laws.
- If a reason arises to completely remove a client and the client's data from the HMIS database, a request must be forwarded to the System Administrator, who will review the request with and obtain the HMIS User Group's approval prior to the client's permanent removal of all the client's information. All client confidential information will remain restricted while the HMIS User Group reviews the appropriateness of removing the client.
- Control release of medical information by giving advance consent prior to disclosures of health information, seeing a copy of health records, requesting a correction to health records, obtaining documentation of disclosures of health information, obtaining an explanation of privacy rights and being informed of how information may be used or disclosed. (HIPPA Act of 1996)

IV – SOFTWARE SUPPORT

Hours of System Operation

Policy: The HMIS System Administrator and Bowman Internet technical staff assures a minimal database down time and posts all scheduled back up and maintenance procedures.

Purpose: To delineate system availability for HMIS Users.

Scope: System wide

Responsibilities: HMIS System Administrator, Database System Technicians

Procedure:

1.0 INTRODUCTION

1.1 HMIS database requires a daily backup of the server and database. The HMIS system operates on the web site twenty-four hours a day/ seven days a week.

2.0 SCHEDULE

2.1 Regular Database Availability:

Twenty-four hours a day, seven days a week, excluding acts of God, or federal and/or a state declared emergency situation.

2.2 Planned Interruption of Service:

2.2.1 Down time is anticipated for data conversions and server maintenance.

2.2.2 HMIS System Administrator posts any scheduled server downtime on the HMIS NewsFlash and/or e-mail/faxes all Agency Administrators one week prior to scheduled down time.

2.2.3 Agency Administrators must reply back with response; otherwise HMIS Technical Support Staff will phone all non-responders.

2.2.4 All posted downtime communication includes an explanation of the purpose and the expected benefits/consequences thereof.

2.2.5 Provider Agencies formulate and publish a manual back-up plan for maintaining client intake, information and services during any interruption of service.

2.2.6 HMIS System Administrator notifies all Agency Administrators via e-mail or fax when service resumes.

2.3 Unplanned Interruption of Service:

2.3.1 Advanced notice of unplanned interruption of service may or may not be possible.

2.3.2 HMIS System Administrator notifies all Agency Administrators via e-mail or fax about service interruption.

2.3.3 HMIS System Administrator, HMIS Technical Support staff and Bowman Internet Technical Support staff make a determination of the problem severity and may institute one of the following:

- Repair problem within two hours

- Switch over to a secondary server
- 2.3.4 Once problem is repaired, HMIS System Administrator notifies all Agency Administrators via e-mail or fax when service resumes.
- 2.3.5 If switched over to a secondary server, the Bowman Technical Support staff will restore production server with latest data from secondary server. This occurs during the next full backup process.
- 2.3.6 HMIS System Administrator and/or HMIS Technical Support staff fills out an incident report.

Technical Support

Policy: The Homeless Management Information System (HMIS) System Administrator oversees HMIS support to all active Provider Agency staff.

Purpose: To delineate a sequence for End-users to communicate their questions, database problems and suggestions to the HMIS System Administrator.
To document the resolution of HMIS calls and e-mails.
To ensure quality control over technical support services.

Scope: HMIS End-users.

Definitions: *Provider Agency:* An agency authorized to participate in the HMIS.

End-user: Any person given access to the database including staff and volunteers.

Error: A documentable occurrence that prevents an End-user from proceeding further.

Deficiency: An insufficiency in the software application.

Performance: The lack of execution and/or operation of the software.

Technical Support Staff: Include, in ascending order, Help-desk personnel, Application Specialist, HMIS System Administrator and Bowman Internet System's Help desk personnel.

Responsibilities: HMIS System Administrator and HMIS Technical Support Staff.

Procedure:

1.0 INTRODUCTION

HMIS Help Desk staff provides an efficient, professional resource for an End-user to ask questions, report problems and make suggestions in regard to the HMIS computer system.

2.0 NON-EMERGENCY ISSUE TECHNICAL SUPPORT

2.1 Non-emergency issues including questions, technical/task assistance, data correction, training concerns, reportable database problems and suggestions for future enhancements. (For emergency issues/problems, contact Agency Administrator and have him/her use the Rapid Response Technical Support Policy.)

2.1.1 An End-user attempts to solve an issue through the following sequence:

1. Checking the HMIS user manual.
2. Checking the on-line Help manual.
3. Asking HMIS End-users within the Provider Agency.

4. Asking Agency Administrator.
 5. Asking HMIS End-users from other Provider Agencies.
 6. E-mailing HMIS Technical Support staff.
 7. HMIS Technical Support staff responds within 24 hours via e-mail Monday through Friday 8:00 a.m. to 5:00 p.m. Arizona Time.
- 2.1.2 If the issue is not resolved with the above resources, then the Agency Administrator/Executive Director calls the HMIS toll-free telephone number.
- Hours of operation: 8:00 a.m. to 5:00 p.m. Arizona time.
 - HMIS Technical Support staff assists each call on a first come, first serve basis.
 - HMIS Technical Support staff enters each call into a software support database to track call information.
- 2.1.3 Provider Agencies report all HMIS database incidents to the Help Desk within 24 hours of occurrence.

3.0 HMIS TECHNICAL SUPPORT STAFF ANALYSIS OF NON-EMERGENCY REQUESTS

3.1 Request categorization and action.

Each request will be categorized and an action will result from that specific request.

Type of Call	Category	HMIS Technical Support Staff
Basic Questions	Technical/Task Assistance Data Correction	Guides End-user through assistance process. Documents correction request and contacts System Administrator.
	Training Issue	Documents issue.
Software Problem	Error	Documents error and starts Software Correction Procedure.
	Deficiency	Documents deficiency and reports to System Administrator.
	Performance	Documents performance and starts Performance Correction Procedure.
Request for Software Improvements	Design Changes Integration	Documents request. Documents request, sends out Data Integration Request Form.
	Enhancements	Documents request.

- 3.2 Technical Support staff enters incident into a software support database, which includes the agency and caller's name, date, time, request and action taken.
- 3.2 Technical Support staff, at the end of every month, compiles and reports all categories of calls and reviews correspondences with the HMIS System Administrator.
- 3.3 HMIS System Administrator and HMIS User Group review monthly End-user suggestions and comments and determine what, if any action is needed.

4.0 TRACKING END-USER SATISFACTION

- 4.1 Periodically, the HMIS Staff randomly surveys End-users about Technical Support Quality and sends report to HMIS System Administrator.
- 4.2 HMIS System Administrator and HMIS User Group review quarterly End-user Support Survey and determine what, if any action is needed.

Rapid Response Technical Support

- Policy:** HMIS technical support staff and Bowman Internet Systems (BIS) provide emergency database technical support to HMIS Provider Agencies.
- Purpose:** To define the conditions justifying “rapid response support”, outline the procedure for communicating the request and the procedure for documenting and assessing outcome.
- Scope:** HMIS System Administrator, HMIS technical support staff, Bowman Internet Systems and Provider Agency Administrators/Executive Directors
- Standards:** HMIS technical support responds by phone within *15 minutes* to only the Provider Agency Administrator, Agency Executive Director or System Administrator and notifies Provider Agency contact and System Administrator of action plan and resolution within 1 hour. Bowman Internet Systems offers 24 hours service when HMIS support service is not available.
- Definitions:** *Provider Agency:* An agency authorized to participate in the HMIS.
- Responsibilities:** HMIS technical support staff.

Procedure:

1.0 INTRODUCTION

HMIS database support center (Help Desk) responds to all emergency circumstances regarding the Maricopa HMIS computer system, which require a quick and efficient response.

2.0 RAPID RESPONSE CONDITIONS:

Any major system or component failure, which proves critical to an HMIS Provider Agency’s business practice, constitutes a condition for rapid response.

3.0 CONTACTING TECHNICAL SUPPORT:

3.1 Monday through Friday between 8:00 a.m. to 5:00 p.m. Arizona Time:

The Agency Administrator/Executive Director reports problem to the HMIS toll-free telephone number. Each call will be assisted on a first come, first served basis.

3.2 All other hours:

3.2.1 The Agency Administrator/Executive Director

- Contacts the System Administrator via cell phone *and*
- Contacts Bowman Internet System (BIS) at 1-888-580-3831.
 - Dials #520 after pre-recorded messages starts.
 - Leaves contact information and a detailed message of the problem.

3.3.2 BIS support staff promptly returns the phone call and begins recovery procedures based on the Severity Code Response Times below:

Severity Level	Description	Bowman Systems Response
1	Major system or component is inoperative which is critical to the CI&R's business	Initiate problem resolution within 1 hour of discovery or notification, whichever comes first and notify CI&R of action plan and resolution within 2 hours of discovery or notification, whichever comes first.
2	CI&R is impacted by service delay but is still able to maintain business functions.	During BIS normal business hours, BIS will initiate problem resolution within four hours and notify CI&R of action plans and resolution within 6 hours of discovery or notification, whichever comes first.
3	The problem has a reasonable circumvention and the CI&R can continue with little loss of efficiency.	During BIS normal business hours, initiate problem resolution within eight hours and notify CI&R of action plans within 12 hours of discover or notification, whichever comes first.
4	The call requires minor action or is for informational purposes only.	Response time within 24 hours of discovery or notification, whichever comes first.

3.3 Email Notifications:

Although e-mail may be used *after* initial contact, e-mail is not an appropriate method for communicating rapid response needs. Both parties, support staff and the agency administration, must agree to the use of e-mail as a follow-up communication method.

4.0 PROCESSING OF THE ISSUE/PROBLEM

Responsible Party	Duties
Provider Agency Administrator, Agency Executive Director, or System Administrator	<ul style="list-style-type: none"> • Reports problem to the HMIS via a toll-free telephone number.
HMIS Technical Support or BIS staff	<ul style="list-style-type: none"> • Responds by phone within 15 minutes to only the Provider Agency Administrator, Agency Executive Director or HMIS System Administrator. • Notifies HMIS System Administrator by phone. • Contacts necessary parties, which may include Bowman Internet Technical Support. • Institutes an action plan and resolution within 1 hour of initial contact.
HMIS System Administrator	<ul style="list-style-type: none"> • Assists HMIS Technical Support or BIS staff in resolution of issue.
HMIS Technical Support or BIS staff	<ul style="list-style-type: none"> • Works with the Agency Administrator/Executive Director until the issue is resolved. • Logs all correspondences including specific date, nature of call and outcome of correspondence. • Documents final resolution. • Sends brief report to HMIS System Administrator.
HMIS System Administrator	<ul style="list-style-type: none"> • Assesses resolution. • Determines if future preventative measures need to be addressed. • Issues monthly report to HMIS User Group.
HMIS Technical Support	<ul style="list-style-type: none"> • Fills out computer generated contact log sheet, which includes agency name, the date, time, issue/problem, and action taken.
HMIS Technical Support	<ul style="list-style-type: none"> • Compiles and sends the Rapid Response Report to the HMIS System Administrator at the end of every month.
HMIS System Administrator, User Group	<ul style="list-style-type: none"> • Reviews monthly the Rapid Response Report and determine what action, if any, is needed.

V – TRAINING REQUIREMENTS

P&P#: V - 01
Approved by: HMIS User Group

Effective Date: _____
Last Revision Date: _____

Training Requirements – To be Developed

VI – REPORT GENERATION

Reports

Policy: The Maricopa Homeless Management Information System (HMIS) provides maximum reporting flexibility including standardized, agency-specific and system-wide customized reports and guidelines for the release of data.

Purpose: To educate Provider Agencies about reporting responsibilities and procedures.
To set parameters relating to the release of aggregate data to outside sources.

Scope: All HMIS Provider Agencies and End-users.

Definitions: *Client:* Any person who received, applied for or was denied services by a Provider Agency.

Client's guardian: Any person legally responsible for a minor or an adult according to Arizona Revised Statutes (A.R.S.). All references to "client" in this policy also apply to "client's guardian."

Custom Report: A report, which can be created by HMIS Provider Agencies using the ServicePoint Report Writer.

Maricopa HMIS database: The Homeless Management Information System's database, also known as HMIS database and/ or database.

Provider Agency: An agency authorized to participate in the HMIS.

Outside source(s): Organization(s) who are not current HMIS Provider Agencies.

Procedure:

1.0 PROVIDER AGENCY'S RESPONSIBILITIES

1.1 Laws and Regulations:

A Provider Agency will abide by:

- All Federal Confidentiality Regulations including those contained in the Code of Federal Regulations, 42 CFR Part 2 (regarding disclosure of alcohol and/or drug abuse records).
- Health Insurance Portability and Accountability Act of 1996 (HIPPA) when applicable.
- Arizona State laws and Federal laws related to confidentiality and security of medical, mental health and substance abuse information including Arizona Revised Statutes Title 12, Courts and Civil Proceedings and Arizona Revised Statutes Title 36 Public Health and

Safety, and Code of Federal Regulations 42 CFR Part 2 and all other relevant statutes, rules and regulations.

1.2 Report Preparation.

A Provider Agency will:

- For Research Studies and Reports, the provider agency will follow their individual Agency Research Policy. The Agency Administrator will notify the HMIS, submit a request and be approved by the Provider Agency's Human Subjects Review Committee or a similar committee (if such a committee exists within the Provider Agency) prior to conducting an evaluation or research report.
- Retain access to all Provider Agency's client identifying and statistical data.
- **Not** report or release any identifiable client information on clients that the Provider Agency has not served or obtained a signed Consent to Release Information Form.
- **Not** report on any other Provider Agency's client data unless approved by that Provider Agency (See 2.0 for system wide aggregate data).

1.3 Report Generation and Report Analysis

A Provider Agency will:

- Use database, standardized reports to maintain data integrity and perform business related duties.
- Use the HUD APR to report to HUD.
- **Not** manipulate data or statistics to defraud any person or organization.
- **Not** use database customized reports to inquire into another Provider Agency's data unless written permission is obtained from that Provider Agency.

2.0 SYSTEM WIDE AGGREGATE DATA PROCEDURE

2.1 System wide aggregate data:

- Includes client information from all Provider Agencies or a subset of Provider Agencies participating in the Maricopa HMIS.
- **Does not** include the HUD-APR and standardized reports.
- **Does not** apply to aggregate data produced by a Provider Agency that includes only that Provider Agency's data.

2.2 Creating System wide aggregate data:

2.2.1 A Provider Agency may produce an aggregate in-house report using the Custom Report Writer but **cannot** release the data or report without prior written permission from the HMIS User Group.

2.2.2 A Provider Agency asks and receives permission from the HMIS User Group through the Custom Report Request Procedure.

2.3 Custom Report Request Procedure:

Responsible Party	Duties
Provider Agency	<ul style="list-style-type: none"> • Fills out a Data Request Form (see Appendix) • Submits brief explanation of reason for report requested and to whom the report will be released. • Marks appropriate desired data elements and/or creates a custom query in the Quick Query section of Report Writer. • Submits request and the name of the Quick Query (if produced) to HMIS System Administrator.
HMIS System Administrator	<ul style="list-style-type: none"> • Produces the requested report. • Checks report for confidentiality and security breaches. • Submits report to HMIS User Group, if the report passes confidentiality and security parameters. • OR returns Data Request Form to requesting Provider Agency with the reason the data elements violate confidentiality and security parameters.
HMIS User Group	<ul style="list-style-type: none"> • Receives approved report from HMIS System Administrator • Checks report for consistency with the explanation of the report. • Re-examines the report for confidentiality and security breaches. • Approves report as written and submits report for data download. • If the HMIS User Group disapproves of the report, it will write a response on the Data Request Form and send one copy to Provider Agency and one copy to HMIS System Administrator.
HMIS System Administrator	<ul style="list-style-type: none"> • Downloads report and sends data to Requesting Provider Agency, if request is approved by HMIS User Group. • Facilitates resolution of requested report with the Provider Agency, if the HMIS User Group denies report approval.

2.4 Publishing Requested Customized Data

2.4.1 All Provider Agencies assume the sole responsibility for accurate data reporting and analysis to funding sources.

2.4.2 The User Group, Advisory Board and the CI&R Executive Director must approve all analysis and interpretation of data released to the press or other outside sources excluding funders.

2.5 Custom Report Production Fee

2.5.1 CI&R Executive Director establishes and assesses a custom report production fee to outside source(s).

2.5.2 The HMIS Executive Director and the outside source(s) agree to the amount and payment method prior to custom report production and release.

2.5.3 An outside source requests a report by following the same procedures outlined in 2.1 by substituting the term Outside Source for Provider Agency.

2.6 Custom Report Log

2.6.1 The System Administrator maintains a log of, copies, and production documentation for all custom reports produced.

VII – SOFTWARE DEVELOPMENT

P&P#: VII - 01
Approved by: HMIS User Group

Effective Date: _____
Last Revision Date: _____

Data Conversion – To Be Developed

P&P#: VII - 02
Approved by: HMIS User Group

Effective Date: _____
Last Revision Date: _____

Data Integration – To Be Developed

P&P#: VII - 03
Approved by: HMIS User Group

Effective Date: _____
Last Revision Date: _____

Design Changes – To Be Developed

P&P#: VII - 04
Approved by: HMIS User Group

Effective Date: _____
Last Revision Date: _____

Software Testing – To Be Developed

VIII – SYSTEM HARDWARE

Hardware Acquisition

Policy: Community Information & Referral, Inc. (CI&R) and the System Administrator assist Homeless Management Information System (HMIS) Provider Agencies in acquiring computer hardware on an as-needed basis during the HMIS implementing process. The available funding supplements those agencies with inadequate or obsolete hardware but will not fulfill all of a Provider Agency's computer hardware needs.

Purpose: To define the hardware acquisition process and roles / responsibilities

Scope: All eligible HMIS Provider Agencies.

Background: Funds from HUD SHP grant(s) and the Arizona Department of Housing are available for Maricopa HMIS provider agencies to acquire computer hardware, networking, and Internet access.

Definitions: *Provider Agency*-an agency authorized to participate in the HMIS.

Responsibilities: HMIS technical support staff.

Procedure:

1.0 HARDWARE ACQUISITION PROCESS

HMIS System Administrator	<ol style="list-style-type: none">1. Conducts an inventory of hardware at Provider Agencies prior to implementation of HMIS.2. Summarizes the Provider Agency's inventory results.3. Estimates the total need for hardware, network equipment, and software licenses.
Provider Agency	<ol style="list-style-type: none">1. Completes an Agency Profile form, which includes hardware and network equipment information.
HMIS System Administrator	<ol style="list-style-type: none">1. Conducts an Agency Needs Analysis.2. Discusses with Provider Agency personnel any HMIS implementation concerns and needs including hardware and network equipment.
Provider Agency	<ol style="list-style-type: none">1. Completes a Hardware Request Form if requesting hardware or network assistance. This form documents the request for hardware including servers, personal computers, network equipment, printers and miscellaneous hardware.2. Acknowledges that HMIS is not responsible for ongoing operating costs or replacement costs for the equipment.

	<ol style="list-style-type: none"> 3. Forwards the Hardware Request Form to the HMIS System Administrator.
System Administrator	<ol style="list-style-type: none"> 1. Reviews the Hardware Request and indicates support for the request; i.e. HMIS implementation at the agency is not possible without hardware / communications support. 2. Forwards the request to CI&R Executive Director for review with the Hardware Review Committee.
CI&R Executive Director	<ol style="list-style-type: none"> 1. Reviews request with budget office to determine if funds are available. If so, schedules for review with Hardware Review Committee. If not, returns to the System Administrator for discussion with the Provider Agency.
Hardware Review Committee	<ol style="list-style-type: none"> 2. Reviews and may approve all, a portion or a limited number of requested items, or reject the entire request. 3. Submits approved requests to HMIS System Administrator. 4. Contacts Provider Agency with decision. 5. Sets up grievance process if request is denied or modified.
CI&R Executive Director	<ol style="list-style-type: none"> 1. Sends and receives quotes from three different vendors for each item greater than \$1,000.00. 2. Selects a vendor. If the quote is for commonly purchased items i.e. standard desktop personal computers, a blanket purchase order will suffice and a separate quote process is not needed. Uncommon item purchases greater than \$1,000.00 require the quote process. 3. Procures and installs the hardware on the Provider Agency's behalf. 4. Sends vendor invoice to CI&R Accounting Staff.
Accounting Staff	<ol style="list-style-type: none"> 1. Coordinates the receipt of hardware purchase funds from all appropriate grants or funding sources. 2. Sends vendor payment. 3. Maintains all purchase and receipt records for HUD and auditing purposes.
Provider Agency	<ol style="list-style-type: none"> 1. Sends written acceptance to CI&R of all hardware received and installed. 2. Uses provided hardware primarily for HMIS access. 3. Installs appropriate security measures to protect hardware including virus protection software. 4. Requests permission from CI&R before retiring or disposing of HMIS hardware. 5. Understands that HUD retains ownership of HMIS purchased hardware and will notify CI&R if the equipment is no longer functional. 6. Accepts, after initial installation, all responsibility for future hardware maintenance and services.
CI&R IT Staff	<ol style="list-style-type: none"> 1. Maintains an inventory of all hardware provided to agencies for HUD and auditing purposes.

P&P#: VIII - 02
Approved by: HMIS User Group

Effective Date: _____
Last Revision Date: _____

Hardware Replacement – To Be Developed

User Workstation Standards

Policy: All Provider Agencies maintain consistent hardware and software configuration standards.

Purpose: To delineate specific standards regarding the configuration of the Provider Agencies' computer workstations.

Scope: System wide

Responsibilities: Provider Agency Technical Staff

Procedure:

1.0 HARDWARE CONFIGURATION

1.1 All Provider Agency user workstations comply with the following minimum requirements:

- Pentium 133Mhz+ PC, or Macintosh 8.0 or higher
- 32MB RAM
- 2GB+ hard drive
- SVGA monitor
- Mouse
- 56K modem for Internet access. (Recommended high-speed Internet connection: DSL, cable or satellite)

1.2 The Provider Agency technical staff installs, configures, supports and maintains user workstation hardware.

2.0 SOFTWARE CONFIGURATION

2.1 All Provider Agency user workstations comply with the following requirements:

- Microsoft Internet Explorer 5.0+ (recommended for best performance) or Netscape Navigator 4.0+ browser
- Internet connectivity or access to LAN
- Virus protection

2.2 The Provider Agency technical staff installs, configures, supports and maintains user workstation software.

2.3 The Provider Agency may request assistance from the HMIS System Administrator.

3.0 Review of User Work Station Standards

3.1 User workstation standards are reviewed each time the User Group considers conversion to an upgrade of the software.

3.2 The system Administrator provides to the HMIS User Group information regarding any changes to the workstation standards that may be required as a result of upgrading the software.

IX – MARKETING AND GROWTH

P&P#: IX - 01
Approved by: HMIS User Group

Effective Date: _____
Last Revision Date: _____

Application for Admission to HMIS – To Be Developed

P&P#: IX - 02
Approved by: HMIS User Group

Effective Date: _____
Last Revision Date: _____

Public Relations – To Be Developed

APPENDICES

Appendix A: Agency Profile Form

Agency Profile

1. Agency Name and Information

Date Filled Out:

By Whom:

Agency Name: _____

Address (physical) _____

Address (mailing) _____

City: _____

State: _____

Zip code: _____

Telephone: _____

Extension: _____

Fax: _____

General E-mail Address: _____

Web Site Address: _____

2. Project Contact

Who should Symmetric Solutions contact in regard to implementing ServicePoint in your agency?

Name: _____

Telephone: _____

E-mail Address: _____

Best time to call: _____

Extension: _____

3. Project Plan

a. Agency Staff

1. Please list the names of all Directors, Managers and Coordinators who will be using ServicePoint.

Name	Job Title
1 _____	_____
2 _____	_____
3 _____	_____
4 _____	_____
5 _____	_____
6 _____	_____
7 _____	_____
8 _____	_____
9 _____	_____
10 _____	_____

b. Program

1. We will be sending you a Program Profile to complete detailing information on all program and funding sources of the agency.

Pam Hughes mbshughes@gorge.net

800.509.2477

4. Technology

A. Hardware

- 1. Does your agency budget yearly for additional hardware upgrades or new computers?
Yes No
- 2. Does your agency use agency-wide e-mail?
Yes No

B. Software

- 1. Does your agency budget time and money for staff technical training?
Yes No
- 2. Does your agency budget for new software and/or software upgrades?
Yes No
- 3. Does your agency have an agency-wide client database?
Yes No If yes, please answer questions a through g.

a. What information does your agency currently track?

b. What information does your agency not track but should?

STAFF USE:

Does this need to be addressed? Yes No

c. What reports does your agency produce or desire to produce?

- d. How does information flow through your agency?
For example, who collects, inputs, updates and accesses the data?

- e. How does your agency envision adding ServicePoint to this flow?

- f. Does your agency have multiple databases?

Yes No

- g. Should these databases be integrated? Please expound if necessary?

- h. Please use the following space to address any concerns or questions.

STAFF USE:

Comments on any Action Items identified above:

Appendix B: Client Acknowledgement of Data Entry into the Maricopa Homeless Management Information System

**COMMUNITY INFORMATION AND REFERRAL, INC.
MARICOPA HMIS**

**CLIENT ACKNOWLEDGEMENT OF DATA ENTRY
INTO THE MARICOPA HOMELESS MANAGEMENT INFORMATION SYSTEM**

The Maricopa Homeless Management Information System (HMIS) is used by homeless provider agencies to record information about clients that they serve. This information helps the agencies to plan for and provide services to clients. This information also can be shared among agencies, if you, the client, agree in order to improve the coordination and delivery of your services.

By signing this document you are:

- Acknowledging that demographic information about you and your family will be entered into the Maricopa Homeless Management Information System (HMIS) database
- Allowing basic demographic information about you / your family to be viewed by other homeless provider agencies. This includes name, age and social security number. Sharing of this information will allow you to be served by other agencies without repeating basic information about yourself / your family. IF THERE IS A REASON THAT PROVIDING YOUR NAME / NAME OF OTHER MEMBERS OF YOUR FAMILY WOULD PLACE YOU / YOUR FAMILY MEMBER AT RISK, PLEASE CHECK HERE TO REQUEST THAT THIS INFORMATION NOT BE SHARED WITH OTHER AGENCIES (A list of the agencies who may be provided is information can be provided by the person reviewing this form with you or can be viewed on the Maricopa HMIS Project Website, Contacts page at www.cirs.org/hmis/contacts.html.)

- No confidential information such as health, medical needs, mental health, and domestic violence will be shared about me without my specific written approval.

Client's Signature

Other Party
(if client is minor or otherwise requires guardian)

Date Signed

Relationship to Client

Effective Date

Appendix D: Computer Security Incident Report

Computer Security Incident Report*

Date: _____

A computer security incident was detected / observed / discovered on _____
(circle one) (enter date, time)
at _____.
(physical location)

Type of Security Incident: The nature of the security incident was (Check all that apply.):

- Unauthorized access to HMIS database.
- Unauthorized disclosure or use of a password
- Alteration of data or computer resources
- Other: (Explain)

Confidentiality of Data:

- Client Information
- HMIS Information
- Other: (Explain)

Impact of Security Incident: The effect of the security violation included the following: (Check all that apply.)

- Disclosure of Data
- Destruction and/or modification of data and/or resource information
- Other: (Explain)

First and Last Name

Signature

Appendix E: Corrective Action Plan Format

Corrective Action Plan

Date of Notification: _____

Name of Provider Agency: _____

End-user (s) (when applicable) _____

Itemized violations

Applicable Document**

- 1. _____
- 2. _____
- 3. _____
- 4. _____
- 5. _____

Itemized Corrective Measures

Expected Completion Date

- 1. _____
- 2. _____
- 3. _____
- 4. _____
- 5. _____

HMIS Resources

Contact HMIS Staff Name and Number

- 1. _____
- 2. _____
- 3. _____
- 4. _____
- 5. _____

First and Last Name
Agency Administrator/Executive Director

Signature

** (Code of Ethics, Agency Partnership Agreement, HMIS Policy & Procedures)

Send to the following address:

HMISsupport@cox.net

Or Mail to:

HMIS System Administrator
Community Information & Referral, Inc.
1515 E. Osborn Road
Phoenix, AZ 85014

Appendix F: Custom Report Request Form

MARICOPA HMIS CUSTOM REPORT REQUEST FORM

Provider Agency Name / Requestor's Organization Name: _____

Requestor Contact Information:

Name of Requestor: _____

Phone Number: _____

E-mail Address: _____

General Information:

Report Name: _____

Purpose of the Report: _____

Time Period: From _____ (MM / DD / YY) to _____ (MM / DD / YY)

Due Date): _____
(specify the date on which the report is needed)

Report Distribution:

Internal to the Agency External to the Agency

If external: please identify the intended recipients: _____

If internal: please identify how often report will be used:

Daily Weekly Monthly Semi-Annualy Annually One-Time Use

Report Content:

Data elements to be included: (Examples are Gender, Ethnicity, Race, Age, Disabilities, Employment Status, Income, etc... If possible attach an example of how the report should look)

1.	3.	5.
2.	4.	6.

Which data element above should this report be sorted by? _____

Export format: Please specify the electronic format in which you would like to receive the report (Note: All custom reports are issued in Read Only format)

Signature:

Agency Administrator Signature

Date

Or If not being requested by a Provider Agency, the signature of the Requestor

Requestor

Date

Send request to the following address: HMISsupport@cox.net

Or Mail to:

HMIS System Administrator
Community Information & Referral, Inc.
1515 E. Osborn Road
Phoenix, AZ 85014

System Administrator Use Only:

The request for a Custom HMIS Report has been reviewed and the data being requested can be provided by HMIS:

The request is from an individual who **does** or **does not** (circle one) represent a provider agency or a funder of HMIS.

System Administrator Signature

Date

User Group Response: Approved Not Approved (If not approved, state reasons)

Final Disposition:

Report Issued on: _____ (Date)

Report placed on the HMIS web site on: _____ (Date)

Appendix G: Agency Reports

Basic Entry/Exit – This report is for those programs that are not funded by HUD, yet have a need for the same type of information that is generated for the HUD 40118 APR report. The Basic Entry/Exit report generates a “HUD APR-like” report for the program and date range you have selected. The data for this report is captured in the same method as the HUD APR but pulls instead from the Basic Entry/Exit worksheets of a client’s record. Note that the supportive services reported in the APR will be displayed only if the client’s HUD worksheet has an exit date and the “program providing” is captured in the service provided section of applicable services recorded.

Clients Served – The Clients Served Report gives an unduplicated count of clients your agency/program has served within a certain time period. The report checks ALL service related information for data that was either created or provided by your agency/program (this includes service items or shelter stays). This is an unduplicated report with distinct clients only being counted once. This report uses the “unique id” system mentioned above to eliminate counting clients who have been entered into the system more than once. The unique id system works off of the client’s first name, last name, sex and date of birth. (Note: The unique id for Anonymous clients is handled a little differently, making each one always unique.)

The counts are broken down various ways to cover a wide range of reporting needs for various agencies. The “old” counts check to see if a client has been helped by your agency/program prior to the reporting date range specified. When checking for old client, the report goes back a timeframe equal to the number of days you’re currently reporting on. For example, with a date range that spans 30 days, the report will consider a client “old” if that client was helped by your agency/program in the 30 days prior to the report start date. The “new” doesn’t necessarily mean that the client was not in the system before, but rather the client has not been worked with in the period of time prior and equal to the data range specified in the report. Note: The “Total Families Served” and “Average Family Size” totals are based on the actual number of family members helped. So, there may be some overlap in the old and new Total Families Served counts.

Daily Bed Report – This report allows you to generate a daily bed list report of which clients stayed in what bed on a specific night. Select options for date, program and sort by either bed number or last name. The report will give you a list of information for the program identified including bed number, client name, date of birth, gender, social security number and check out status as of to date identified in the criteria. This criterion includes a date range, which results in several days’ information with previous and next day links to page through each day’s bed stays. The “sort by” option Service Family ID sorts the client list by family groups. There’s also a “# in Family” count displayed when you use this sorting option. Totals have been added for each bedlist for “Beds in use” (the person is still in the bed as of midnight), new Check Ins and Check Outs. These totals are also calculated into a grand total for all the bedlists combined.

HUD 40118 APR - The report generates the HUD APR for the program and date range you have selected. The data for this report comes from the HUD APR worksheets that are entered on each client that received services. You will have to download the latest version of the report from www.hud.gov to copy the ServicePoint response over to and submit to your funder. Note that the supportive services reported in the APR will be displayed only if the client’s HUD worksheet has an exit date and the “program providing” is captured in the service provided section of applicable services recorded.

Referral – This report allows you to generate a list of referrals made or received by your agency for a specified date range and program. Referrals reports can be generated by either date created or date provided. The date created is the date the referral was actually entered into the system or the date a user identifies the need. The date provided is the date that can be captured in the “services provided” section of a service item and is intended for recording the date that the referral was actually made.

Appendix H: Systemwide Reports

All Reports function like their Agency level counterparts, except client identifying fields are not listed and there are no links to any records displayed. All of the reports have various options – for example, an agency can select a date range for their report.

Downloads (perform downloads during off hours or periods of low system usage)*

System Admin II has the ability to download 2 items: Printed Directory and ServicePoint Tables. The Printed Directory is in standard html format with indexes for Taxonomy, Agencies, and Programs. This information can be used to create a printed directory for all agencies and programs except the ones who have “No” entered in their profile for Print in Directory option.

The ServicePoint Tables option allows System Admin II to download information from the various database tables within ServicePoint.

Appendix I: Hardware Request Form

Agency	
Agency Name	
Address	
Contact	

Servers		
Purpose: _____	Processor: _____	Monitor: _____
Quantity: _____	Memory: _____	CD/DVD: _____
Location: _____	HDD: _____	Tape: _____
	Mounting: _____	UPS: _____

Personal Computers		
Purpose: _____	Processor: _____	Monitor: _____
Quantity: _____	Memory: _____	CD/DVD: _____
Location: _____	HDD: _____	Tape: _____
	OS: _____	Software: _____

Network Equipment		
Purpose: _____	Routers: _____	DSL Modems: _____
Quantity: _____	Hubs/Switches: _____	Cable Modems: _____
Location: _____	Patch Panels: _____	NIC Cards: _____
Service: _____	Cabling: _____	Other: _____

Printers & Other Equipment		
Purpose: _____	LaserJet: _____	Other: _____
Quantity: _____	Inkjet: _____	Other: _____
Location: _____	Other: _____	Other: _____

I understand that if approved, this is a one time purchase and Maricopa HMIS is not responsible for ongoing costs of operating the equipment / communications connection or replacement of requested equipment.

Signature: _____ Date: _____
 Provider Agency Executive Director

System Administrator Use Only:

I have reviewed the hardware request and agree that the provider agency is not able to implement HMIS without the above requested equipment.

Signature: _____ Date: _____
System Administrator

Reviewed and Approved by: _____ Date: _____
Community Information & Referral, Inc.

Appendix J: HMIS Code of Ethics

Code of Ethics for Persons Using the CI&R/HMIS

As a User (agency staff or agency volunteer) of the HMIS who enters information into the HMIS or views electronic information in the HMIS, I agree to the following:

_____ I understand that my User ID and Password give me access to the Maricopa HMIS.

_____ My User ID and Password are for my use only and I will not share, or allow them to be shared, with any person for any reason.

_____ I will take all reasonable means to keep my User ID and Password physically secure to prevent its use by any other person.

_____ I understand that the only individuals who can view information in the Maricopa HMIS are authorized users and the clients to whom the information pertains.

_____ I understand that not all users can view all information.

_____ I will only view, obtain, disclose, or use the database information that is necessary to perform my job.

_____ If I am logged into the Maricopa HMIS and must leave my work area for any length of time, I must log-off the Maricopa HMIS and close the Internet browser before leaving the work area.

_____ A computer that has Maricopa HMIS open and running shall never be left unattended by the person with the authorization to use that computer.

_____ Failure to log off the Maricopa HMIS appropriately may result in a breach in client confidentiality and system security.

_____ I will obtain and file a hard copy of such client consent forms as are required by my agency, state and/or federal law and the Maricopa HMIS.

_____ I understand that I must save data at regular intervals because the system will log off at 15-minute intervals without automatically saving the information that I have entered.

_____ I agree to enter data into the Maricopa HMIS in accordance to the policies of my agency and the standards of the Maricopa HMIS.

_____ I agree that I will not enter in the HMIS discriminatory comments made by or about an employee, volunteer, or other person based on race, color, religion, national origin, ancestry, handicap, age, sex, and sexual. I understand that offensive language and profanity are not permitted in the Maricopa HMIS. This does not apply to the input of direct quotes by a client IF the Agency believes that it is essential to enter these comments for assessment, service and treatment purposes.

_____ I agree to use the HMIS ONLY for business purposes related to serving the clients of my agency.

_____ If I notice or suspect a security breach, I shall immediately notify the designated HMIS Contact person in my agency or the CI&R System Administrator.

_____ As a Maricopa HMIS user, I will treat other Member Agencies and their staff with respect, fairness and good faith.

_____ As a Maricopa HMIS user, I will treat clients and potential clients of my agency and other agencies with respect, fairness and good faith in obtaining and entering their data.

_____ As a Maricopa HMIS user, I will maintain high standards of professional conduct.

_____ As a Maricopa HMIS user, I recognize that my primary responsibility is to my client.

_____ I understand that I may be subject to personnel action, including but not limited to termination from employment or volunteer status, from my employer for failure to comply with this Code of Ethics.

I have read, understand and agree to comply with all of the statements above.

Agency User Name and Job Title

Date

Agency / System Administrator Name

Date

Appendix K: Rescinding Client Consent

Maricopa HMIS

Rescinding Client Consent Form

I _____ hereby rescind my consent to _____
Print Client Name Provider Agency

to share basic demographic information (name, Social Security Number and age) about me and my family with other homeless service providers.

I understand that this request to rescind my consent to release information only applies to the provider agency listed above. If I have been seen by other provider agencies, I must also complete this form at the other agencies.

Optional Question: The reason I am rescinding my consent is: _____

Client (or guardian) Signature Date

Signature of Agency Personnel Date

Send a copy of this form to the following address:

HMISsupport@cox.net

Or Mail to:

HMIS System Administrator
Community Information & Referral, Inc.
1515 E. Osborn Road
Phoenix, AZ 85014

System Administrator Use Only:

The request to rescind client consent has been activated as of _____ (Date)

System Administrator Date

Appendix L: Audit Reports

ServicePoint has the ability to internally track client-related activity with an Audit Trail. If this option is set on your system, any time client information is added, edited, deleted, or viewed by a ServicePoint user, that information will be logged. This information can be viewed by Agency Administrators and above in the following reports.

Client/Service Information – This report generates a listing of actions specific to either a user or client within an agency or program. The audit information including actions of add, edit, delete, and view specific for a client and date range.

Access Report: Client/Service Information – The audit access report “audits” the auditor. It lets you see who has been running “Audit report: client/service information” report. It lets people know that the audit reports they are running/viewing are being tracked internally in the system. This should help curb viewing of information for personal gains.

Appendix M: Standard Data Requirements

The Department of Housing and Urban Development (HUD) issued proposed data standards for Homeless Management Information Systems in July 2003. Although those standards have not yet been finalized by HUD, the following provides information about the proposed standards.

- A. Universal data elements – these elements are to be collected from all clients served by all programs reporting to the HMIS:
- Name
 - Social Security Number
 - Date of Birth
 - Ethnicity and Race
 - Gender
 - Veteran Status
 - Residence Prior to Program Entry
 - Zip Code of Last Permanent Address
 - Month and Year Person Left Last Permanent Address
 - Program Entry Date
 - Program Exit Date
 - Unique Personal Identification Number
 - Program Identification Number
 - Program Event Number
 - Household Identification Number
- B. Program-level data elements – these elements are to be collected from clients served by programs that include an assessment of client’s needs as a basic element in their provision of service.
- Income and Sources
 - Non-Cash Benefits
 - Physical Disability
 - Developmental Disability
 - General Health Status
 - Pregnancy Status
 - HIV / Aids Status
 - Behavioral Health Status
 - Domestic Violence
 - Education
 - Employment
 - Veterans
 - Services Received
 - Destination
 - Follow-up After Program Exit
 - Children’s Education
 - Other Children’s Questions
 - Child’s Physical Disability
 - Child’s Developmental Disability
 - Child’s General Health Status
 - Services Received
 - Destination