

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 Referrals</i>						X	X	X		X	X
<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.