MARICOPA ASSOCIATION of GOVERNMENTS
302 North 1st Avenue, Suite 300 ▲ Phoenix, Arizona 85003
Phone (602) 254-6300 ▲ FAX (602) 254-6490

August 24, 2016

TO: Members of the Maricopa Regional Continuum of Care Board

FROM: Kevin Hartke, Councilmember, City of Chandler, Co-Chair
Darlene Newsom, UMOM New Day Centers, Co-Chair

SUBJECT: MEETING NOTIFICATION AND TRANSMITTAL OF TENTATIVE AGENDA

Meeting - 1:30 p.m.
Monday, August 29, 2016
MAG- 2nd floor Ironwood Room
302 N. 1st Avenue
Phoenix, AZ 85003
(Parking is available from the garage below the building. Bring your parking ticket to the meeting for validation.)

The next Maricopa Regional Continuum of Care Board (CoC Board) meeting will be held at the time and place noted above. Members of the CoC Board may attend either in person or by phone. Supporting information is enclosed for your review.

The meeting agenda and resource materials are also available on the MAG website at www.azmag.gov. In addition to the existing website location, the agenda packet will be available via the File Transfer Protocol (FTP) site at: ftp://ftp.azmag.gov/ContinuumOfCareRegionalCommitteeonHomelessness
This location is publicly accessible and does not require a password.

Please park in the garage underneath the building. Bring your ticket to the meeting, parking will be validated. For those using transit, the Regional Public Transportation Authority will provide transit tickets for your trip. For those using bicycles, please lock your bicycle in the bike rack in the garage.

In 1996, the Regional Council approved a simple majority quorum for all MAG advisory committees. If the Continuum of Care Board does not meet the quorum requirement, members who have arrived at the meeting will be instructed a legal meeting cannot occur and subsequently be dismissed. Your attendance at the meeting is strongly encouraged.

Pursuant to Title II of the Americans with Disabilities Act (ADA), MAG does not discriminate on the basis of disability in admissions to or participation in its public meetings. Persons with a disability may request a reasonable accommodation, such as a sign language interpreter, by contacting the MAG office. Requests should be made as early as possible to allow time to arrange the accommodation.

If you have any questions, please call the MAG office.

MARICOPA REGIONAL CONTINUUM OF CARE (CoC) BOARD
TENTATIVE AGENDA
August 29, 2016

	COMMITTEE ACTION REQUESTED
1. Call to Order	
2. Call to the Audience An opportunity will be provided to members of the public to address the Continuum of Care (CoC) Board on items not scheduled on the agenda that fall under the jurisdiction of MAG, or on items on the agenda for discussion but not for action. Citizens will be requested not to exceed a three minute time period for their comments. A total of 15 minutes will be provided for the Call to the Audience agenda item, unless CoC Board requests an exception to this limit. Please note that those wishing to comment on agenda items posted for action will be provided the opportunity at the time the item is heard.	2. Information.
3. Approval of Consent Agenda Prior to action on the consent agenda, members of the audience will be provided an opportunity to comment on consent items that are being presented for action. Following the comment period, Board members may request that an item be removed from the consent agenda. Consent items are marked with an asterisk (*).	3. Approval of the Consent Agenda.

ITEMS PROPOSED FOR CONSENT*

*3A. Approval of the July 18, 2016 CoC Board Meeting Minutes The draft minutes for the July 18, 2016 meeting are posted with the meeting materials.	3A. Approve the CoC Board meeting minutes of July 18, 2016.

*3B. Order of Priority in CoC Program-funded Permanent Supportive Housing

On July 25, 2016 the U.S. Department of Housing and Urban Development (HUD) issued a Notice on Prioritizing Persons Experiencing Chronic Homelessness and Other Vulnerable Homeless Persons in Permanent Supportive Housing. In the notice, HUD urges communities to adopt the order of priority, as outlined in the notice. (Please refer to the attached notice.) This item was brought to the attention of the Coordinated Entry Oversight Work Group (CEOWG) for review and discussion. This item is to recommend that the Board adopt HUD's order of priority in CoC Program-funded Permanent Supportive Housing.

3B. Adopt HUD's Order of Priority in CoC Program-funded Permanent Supportive Housing.

*3C. Maricopa Regional Continuum of Care Strategic Plan to End Homelessness

The workgroup to develop the Maricopa Regional Continuum of Care Strategic Plan to End Homelessness is recommending approval of the draft plan. The draft Strategic Plan to End Homelessness was distributed with the meeting materials.

3C. Approve the Strategic Plan to End Homelessness.

*3D. Coordinated Entry Oversight Work Group-Membership

On February 22, 2016, the Board adopted a Coordinated Entry Oversight Work Group membership policy to ensure adequate representation on CEOWG. CEOWG recently had two resignations: Theresa James and Karia Basta. The group is proposing to add: Jeff Willgale, Veterans Administration; Margaret Kilman, Maricopa County; Riann Balch, City of Phoenix; and, Amy Jacobson, City of Chandler.

3D. Approve new members of the Coordinated Entry Oversight Work Group.

*3E. HMIS Policies and Procedures

The Performance Standards and Data Quality Work Group (PSDQ) have been working with CIR since to finalize the HMIS Policies and Procedures. Attachment of the Policies is required in the 2016 NOFA submission. PSDQ and HMIS have reached consensus on the draft and the Policies and Procedures were presented to the HMIS Committee. A copy of the Policies and Procedures was distributed with the meeting materials.

3E. Approve the HMIS Policies and Procedures as recommended by PSDQ.

ITEMS PROPOSED TO BE HEARD

4. Continuum of Care Updates

MAG staff will update the Board on priorities and upcoming issues.

4. Information and discussion.

5. Approval of the 2016 Continuum of Care Program Project Listing

The Ranking and Review Panel will present the draft 2016 Continuum of Care Program project listing for approval to submit with the 2016 consolidated funding application to HUD. The Ranking and Review Panel carefully reviewed all project applications and conducted project presentations with each project on August 18 and August 19, 2016. The project listing recommendation will include Tier One and Tier Two projects, consisting of renewal projects, new projects created from reallocation, and new Permanent Housing Bonus projects. Please refer to the attached project listing.

5. Approval of the 2016 Continuum of Care Program Project Listing.

6. Continuum of Care Planning Grant Application

MAG Staff will provide a summary of the 2016 Continuum of Care Planning Grant application for information and discussion.

6. For information and discussion.

7. Board Membership Selection Workgroup

On June 27, the Board approved the membership selection process. Staff have

solicited volunteers from the Board, the CoC Committee, PSDQ, and the CEOWG to serve on the selection workgroup. The membership workgroup followed the approved process and

sought letters of interest for new Board members. The workgroup met on August 3, 2016 and is recommended the Board amend the selection process to require resumes and more detailed information and to allow for additional time to seek new membership. A draft change to the Governance Charter was distributed with the meeting materials.

7. Information, discussion, and possible action to amend the Board membership selection process.

8. Request for Future Agenda Items

Topics or issues of interest that the MAG Continuum of Care Board would like to have considered for discussion at a future meeting will be requested.

8. Information and discussion.

9. Comments from the Board

An opportunity will be provided for Continuum of Care (CoC) Board members to present a brief summary of current events. CoC Board members are not allowed to propose, discuss, deliberate or take action at the meeting on any matter in the summary, unless the specific matter is properly noticed for legal action.

9. Information only.

Adjournment.

MINUTES OF THE
MARICOPA ASSOCIATION OF GOVERNMENTS (MAG)
CONTINUUM OF CARE BOARD
July 18, 2016
MAG Office Building, Saguaro Room

MEMBERS ATTENDING

Brad Bridwell, Cantwell Anderson-Cloudbreak
Moises Gallegos, City of Phoenix
Marisue Garganta, Dignity Health
Scott Hall, Community Bridges Inc.
Kevin Hartke, City of Chandler, Councilmember, Co-Chair
*Theresa James, City of Tempe
Bruce Liggett, Maricopa County
Darlene Newsom, United Methodist Outreach Ministries (UMOM) New Day Center, Co-Chair
Amy Schwabenlender, Valley of the Sun United Way (VSUW)
Diana Yazzie-Devine, Native American Connections

*Neither present nor represented by proxy.
#Attended by telephone conference call.
+Attended by video conference.

OTHERS PRESENT

Billie Cawley, CASS
Kelli Donley, AHCCCS
Alfred Edwards, DES
Charlene Flaherty, Corporation for Supportive Housing (CSH)
Walt Gray, Westside Town Hall
Margaret Kilman, MCHSD
Karen Kurtz, Community Bridges Inc., (CBI)
Nancy Marion, House of Refuge
Suzie Martin, Homeward Bound
Lisa Miller, UMOM
Stephen Serrato, Southwest Behavioral & Health
Chela Schuster, UMOM
Nicky Stevens, Save the Family
Charles Sullivan, Arizona Behavioral Health Corp., (ABC)
Jacki Taylor, Save the Family
Michelle Thomas, Community Information and Referral (CIR)
Keith Thompson, Phoenix Shanti
Craig Tripkin, CASS & AHI
Kim Van Nimwegen, VSUW
John Wall, Arizona Housing Inc., (AHI)
Dr. Williams, Southwest Behavioral & Health

Brande Mead, MAG
Maria Piña, MAG
Anne Scott, MAG

1. Call to Order and Introductions
   Darlene Newsom, UMOM, Co-Chair of the Continuum of Care (CoC) Board, called the meeting to order at 2:05 p.m. Introductions of the Board and audience proceeded.

2. Call to the Audience

Audience members were given an opportunity to address the Committee on items that were not on the agenda that are within the jurisdiction of MAG, or non-action agenda items that are on the agenda for discussion or information only. There were no comments from the audience.

3. Approval of Consent Agenda

Addressing the first order of business, Co-Chair Newsom opened the floor to the public for comments on the consent agenda. A correction in the minutes was requested by Amy Schwabenlender, Valley of the Sun United Way (VSUW). The correction now reflects that Co-Chair Newsom, not Marisue Garganta, Dignity Health, requested a second term. She also pointed out that the CEOWG Membership draft was missing. Anne Scott, MAG, apologized that the document was missing from the membership packet, but offered to print out and provide later in the meeting. Ms. Garganta motioned to approve the consent agenda items. Kevin Hartke, City of Chandler, seconded the motion. The motion passed unanimously.

4. Continuum of Care Updates

Ms. Scott provided an update with the points listed below:

- Plans are proceeding for the clients impacted by the HUD decision. MAG has been informed that plans are in place with VSUW, UMOM and New Leaf to assist some families who have fallen back into the area of concern. Most clients have been placed or have housing plans and/or in process of successfully being placed in rapid re-housing (RRH) units. Ms. Scott thanked the Family Housing Hub (FHH), VSUW, City of Mesa, and the projects that came together to think creatively for solutions. With the exception of a few families, all clients are in really good shape.
- NOFA:
    - The collaborative effort is tasked with putting together a ranking and review panel. One of the requirements in the panel is to have consistency from year to year, so members from the VSUW, Maricopa County, City of Phoenix, Department of Economic Security (DES) and Glendale were asked to sit on the review panel. Because the group has been tasked with having more members, Corporation for Supportive Housing (CSH), Circle the City, and Arizona Coalition to End Homelessness (AzCEH) were also asked to serve. Maricopa County, City of Phoenix, CSH and Circle the City has committed to join. AzCEH cannot serve because they are a membership organization, and they have conflict of interest requirements that don't allow them to serve. Although the group is waiting to hear from DES, it feels it has a good panel moving forward. Ms. Scott thought it was a good idea to mention who was approached, and who would be serving on the panel. Additionally, she clarified that last year, a member from the City of Mesa sat on the ranking and review panel, but because they currently have a five year project up for renewal, it is unable to serve this year.
    - To accommodate the ranking and review process, the group is proposing moving the August 22nd Board meeting to August 29, which will allow enough time to complete the review process.

- On the plan to end homelessness: a draft was updated and distributed to the Board's subgroup over the weekend. Updates to that draft were received, and MAG staff will meet with graphic designers this week. The group hopes to have the plan adopted at the August Board meeting.

Co-Chair Newsom opened the floor for questions. Moe Gallegos, City of Phoenix, inquired about the families in the area of concern. Ms. Scott replied that she was notified on Friday that all the families were taken care of, and that MAG was able to work with providers to assist with short-term funding to stay in place until their housing plans were finalized. Ms. Scott indicated she spoke briefly with Nancy Marion, House of Refuge, and expressed that there were concerns over a few families at that organization who had fallen out because their housing plans weren't yet finalized. Mr. Gallegos inquired whether there was anything that could be done to help. Ms. Scott expressed that Kim Van Nimwegen, VSUW; Mattie Lord, UMOM; and Kathy DiNolfi, A New Leaf, were working closely on resolving this issue. Ms. Scott deferred to those directly involved, and indicated that her role has been putting together the funding. Ms. DiNolfi indicated that it was her understanding that all families had been identified and connected with services and agencies. She added that as of Friday, everyone was in process. Ms. Marion expressed concern about the August 1 drop deadline for about 12 families at House of Refuge who would be served with an eviction notice, taken to court and relocated. She continued that those families, for whatever reason, are having problems locating homes. There might be a two week delay between August first and mid-August, when House of Refuge can hopefully get them into houses. She inquired where funding would come from for that two week time period. She added that stress is creating some immobility to some families, and they are unresponsive to calls and letters from the agency. The agency continues working with those five families that it's very concerned about. Ms. Marion reiterated that the agency was worried about those 12 families who were in danger of being displaced. Nicky Stevens, Save the Family, indicated that her agency wasn't included as the original providers to assist the families in need, but expressed that they are working with the families and would be happy to work with others so as to not duplicate efforts and to know where the gaps are. She added that Save the Family has a program through the City of Mesa that is providing deposit assistance, security deposits for utilities, and first month's rent, along with the rent from House of Refuge. Ms. Scott thanked Save the Family for being integral in the whole process. Scott Hall, Community Bridges Inc., (CBI) thanked everyone who has stepped up to help.

5. <u>Board Membership Selection Workgroup</u>
Co-Chair Newsom reminded the Board that it had approved the membership selection process on June 27, and advised the group it has volunteers from CoC Committee,
Performance Standards Data Quality (PSDQ), and the CEOWG to serve on the selection workgroup. Co-Chair Newsom indicated that the workgroup would need an additional two members from the Board to serve for a minimal commitment, meeting once during the first

two weeks of August to look through letters of interest and assist in recommending new members. Ms. Garganta and Bruce Liggett, Maricopa County, agreed to serve.
Co-Chair Newsom moved back to discuss the membership policy on the consent agency, which the Board did not have at the beginning of the meeting. Co-Chair Newsom requested a motion to approve the consent agenda. Mr. Liggett approved the motion. Mr. Hall seconded the motion. The motion passed unanimously.

6. Coordinated Entry Oversight Work Group (CEOWG) Recommendation on Center for Hope

Co-Chair Newsom invited Kelli Donley, AHCCCS to speak on behalf of CEOWG. Ms. Donley indicated that several weeks ago, the group was approached by Center for Hope with a proposal for working with coordinated entry in a nontraditional way. She expressed that CBI and Center for Hope have proposed taking one year to figure out how to work with coordinated entry so that Center for Hope can still accept direct referrals from sources outside the traditional coordinated entry mechanisms, such as hospitals and the legal system. After two meetings, the group has decided it would like to move forward and give CBI and Center for Hope a year to continue operating as is. Ms. Donley indicated that the recommendation is that the organizations not lose points for working outside of traditional coordinated entry, when money is considered. CBI proposed trying to increase housing for all pregnant women, not just substance abusing women, and that they would work on that proposal with their board, and report back to CEOWG. Ms. Donley indicated that the work group's proposal is to move forward with the recommendation, recognizing that CBI and Center for Hope have committed to working closely with the FHH and the Human Services Campus to ensure this works as well as possible with the existing coordinated entry process. Ms. Donley recognized that the last time she stood before the Board, she pled with providers and members of the community to participate as much as possible in the coordinated entry process, and to not make these types of exceptions; however, she acknowledged that in coordinated entry, substance abusing pregnant women are a very specific group of people, for which there should be an exception – specifically when there are direct referrals from both hospital or the legal system. Ms. Donley stated that the group would not want those relationships to fall away to meet the coordinated entry model.

Brad Bridwell, Cantwell Anderson-Cloudbreak, inquired about whether it was discussed if CBI would become an access point. Ms. Donley indicated it was discussed, there was no decision made, that there was no formal recommendation on that on this proposal, and that those were details still being worked out for next year. She added that the majority of the workgroup would probably prefer that this all go through the FHH; that the group believes in the Standing Strong for Families work, the FHH, as well as the Human Services Campus. Ms. Donley expressed that substance abusing pregnant women are considered single up until their third trimester, at which point they are considered family. She expressed that determining all

those details with substance abusing women can be difficult, and indicated that the work continues being worked out.

Mr. Bridwell inquired on the likelihood that the FHH would continue to handle all the coordinated entry. Ms. Donley expressed that this was her recommendation, but that this had not yet been decided and that the workgroup was willing to spend the next year working on this particular issue with all the aforementioned providers to come up with the best solution.

Mr. Gallegos inquired whether this was because CBI had not yet developed a protocol, to which Ms. Donnelley replied that this was correct, and that the committee had been working on a draft protocol for a "side door policy". She stated that the workgroup believed that substance abusing pregnant women should be included in that. Mr. Gallegos inquired whether there were other groups that this protocol would apply to. Ms. Donley replied that the group anticipates that other providers will come forward with other populations, but that this subset was the first. She shared that the workgroup would like to have a draft policy within the next two weeks. Mr. Gallegos indicated that everybody was doing very detailed worked, but his concern was that in trying to do things exactly right, we lose sight of some things that just can't fit into one thing. He encouraged all to be mindful of things that don't fit into the box, and asked all to be open-minded in that respect.

Co-Chair Hartke inquired whether the group could put this protocal up against the NOFA application next year. He indicated wanting to be further along next year in the process to help organizations see where they fit and what the process is, and proposed moving the timeline to nine months rather than a year, with the goal that if the group has the process further along, asking this question would no longer be necessary.

Mr. Hall requested to be recused from the vote, but not the discussion. He indicated that nine months was a fair length of time to figure out how coordinated entry would work. Ms. Schwabenlender expressed that when writing the recommendation, it's not updating a policy or procedure over a particular agency or program, but rather, about a subpopulation. She added that it's not so much about having a grace period, but that it's about this particular subpopulation, and that as soon as the policy was written and put into effect, the Board can expect to see it in place.

Ms. Donley agreed, and added that policy has very specific recommendations from the FHH and Human Services Campus on what those exceptions might be.

Co-Chair Newsom opened the floor for comments. Mr. Bridwell moved to accept the recommendation to allow discussions to continue and to exempt Center for Hope from this round of application from any negative point scoring related to coordinated entry participation.

Mr. Gallegos seconded the motion. Mr. Hall abstained from voting. The motion passed unanimously.

7. 2016 NOFA Review

Co-Chair Newsom invited Ms. Scott to provide the NOFA review. Ms. Scott indicated that the NOFA was released June 27, and because applications have yet to be released, the specific questions are unclear, including how they're posed, what is required of providers and collaborative applicants, or any other details. She stated the seven percent of the CoC funds must be placed in Tier 2, which would equal $1.7 million dollars in our Continuum, while $22.8 million would be placed in Tier 1. Ms. Scott stated that the overall annual renewal amount is $24,568,339. She added that while final details aren't available on what will be allowed on the bonus project, a five percent calculation was performed of the preliminary pro rata need which is allowed in the bonus project. She continued that the Continuum will be allowed the opportunity to apply for $897,499 in the bonus project. Ms. Scott pointed out that there were significant differences and similarities in the NOFA. For example, she indicated that the scoring was largely the same, such as Tier 2 projects and the overall Continuum of Care being the bulk of the points, as well as the ranking in Tier 2 being the most important in terms of whether HUD would fund those projects. She added that HUD would look at the Continuum to see whether it has a systemic response to homelessness; how it's incorporating performance measures and creating a coordinated entry system that guarantees that people who need the service the most receive them, and reallocation and system performance. Ms. Scott indicated that measures will be submitted this year into HDX by August 1st, which counts for ten points in the CoC application. She expressed that the Continuum is gathering the necessary data and that the Continuum will be meeting with the projects on Friday whether the application is available on e-snaps or not. The hope is that the application is available so that the group can have a dialogue with the providers and the community about the 2016 NOFA application and its considerations.

Ms. Marion inquired whether there would be an adjustment in the timeline if the application were not out in a timely fashion. Ms. Scott replied that there was a national movement amongst CoCs to request assistance from HUD and to delay the deadline. While HUD has not responded to that request, it has previously delayed the deadline. Ms. Scott added that the Continuum is supportive of the request to extend the deadline.

8. **Program Performance Report–Scorecard Approval**

Co-Chair Newsom invited Ms. Scott and Ms. Lord to present the recommended changes to the scorecard. Ms. Lord began by stating that while the content of the scorecard is the Committee's responsibility, it is PSDQ's responsibility to figure out how those items are calculated, and that the overall approval of the scorecard falls upon the Board. She indicated that after the Board

met in June to discuss the content changes to this year's scorecard, it decided to integrate four new factors:

1. to find a way to integrate as many of the systems levels performance measures as possible;
2. to ensure coordinated entry was folded into the scorecard and participation in the coordinated entry system;
3. to somehow represent the importance of the standards of excellence and the operation of the quality program in addition to the performance measures and finally,
4. to roll in cost-effective measures.

Ms. Lord indicated that following the June meeting, the group created a subcommittee comprised of members from PSDQ and the Committee, which met to integrate those four factors into the scorecard. Ms. Lord expressed that although the group made some headway, it was unable to finish the job. She continued that the modified recommendations came to the Committee again in the July meeting, which resulted in fruitful dialogue with some of the scorecard being approved. Ms. Lord expressed that HUD will calculate the system performance measures differently by measuring the *change in income*, not *maintain or increase.* Ms. Lord continued that a non-scored item placeholder was put in place into this year's scorecard to establish the baseline data, to illustrate to providers the seriousness of the measure, and to demonstrate to HUD that not only are the performance measures understood, but they are trying to be achieved. After examining two different reports presented by Community Information and Referral (CIR), the workgroup chose 0554.01.

Ms. Lord indicated that the second change involved Community Priorities and Standards, where the coordinated entry participation was inserted. She expressed that for the Welcome Center, it would be "cooperation with onboarding schedule"; for example, if an agency had onboarded or was cooperating with the onboarding schedule, they would receive points. For the FHH, it would be based on compliance with the agreement that 85 percent of referrals are accepted from the FHH (or not rejecting more than 15 percent of referrals from the Hub). PSDQ determines that calculation.

The final recommendation was to not monitor a score this year on issues relating to compliance with community adopted standards of excellence. Ms. Lord indicated that because monitoring is not currently in place, this item could not be scored. To illustrate the emphasis to the participating projects and to HUD, a placeholder was indicated for items pertaining to quality programming and the standards of excellence. She added that these items would be scored in the next NOFA. Ms. Lord indicated that for some reason, quite a few points were lost in the last scorecard, and the Continuum wanted to make as many changes to demonstrate it is aligning with HUD's priorities. She stated that although "fair and objective criteria" was used, ten out of 16 points were lost in this category.

Mr. Bridwell inquired about whether income increase could be run and measureable using the 0554.01 report, and if the Continuum was deciding not to do so in place of the maintained or increased income. Ms. Lord expressed that it was her belief it could be run and measured, but was unsure whether it was accurate. She added that income was unstable in HMIS.

Ms. Thomas indicated income would be accurate if ran in HMIS, and that it would show increases in income only. Mr. Bridwell inquired how compliance with community adopted standards of excellence was measured, and Ms. Lord indicated that the monitoring process had not yet been designed. Mr. Bridwell proposed including "accepted community standards" to make it more action oriented to demonstrate it is in the planning process and the box on the scorecard is checked, to which members of the Board agreed. Ms. Lord added that if characters allowed in the narrative, reference can be made in the scorecard.

Ms. Scott indicated there was information on the project ranking review and capacity there are points that will be assigned in the 2016 NOFA.

- Ten points are based on attaching the written documentation demonstrating objective criteria;
- Four points are allotted for showing that a project review and ranking that considers the past performance data;
- Four points are for project review and ranking consideration of the severity of needs experience by program participants;
- Four points are for demonstrating the ability to reallocate low performing projects;
- Three points are if the CoC uses publicly-announced ranking process, publishes policies and procedures and dated meeting minutes regarding competition and finally,
- Four points are for CoC monitoring project performance.

Ms. Scott continued with Part 2 and explained that the process that the Board has adopted includes convening a small group of Committee members and allocating points for the HUD ranking priority and commitment to policy priorities. After meeting Friday afternoon, the group decided to four principles into the scorecard: chronic homelessness, housing first, cost effectiveness, and return to homelessness, which is a system performance measure that is being measured by HUD this year.

For chronic homelessness, the group decided that if a project dedicates (not prioritizes) 100 percent of their turnover to individuals or families experiencing chronic homelessness, they would be eligible for eight points.

For Housing First, the project would receive seven points. That would provide for a total of 15 points in the HUD ranking priorities if the project commits to operating to a Housing First model and indicating a willingness to dedicated beds to the chronic homeless.

Ms. Scott indicated that the question "The project is cost effective compared to other projects funded by CoC funds" would be measured by the average HUD CoC investment per positive housing outcome, the top 25 percent of projects would receive five points, the middle 50 percent would receive three points and the bottom 25 percent would not receive points. In the return to homeless, any project that achieves a 15 percent or less return to homeless rate would be eligible for five points, which would equal ten points for commitments to policy priorities (#10 on the scorecard).

Ms. Garganta inquired about the income improvement project, and how projects would score if they had missing information since the Continuum was going to add the criteria.

Ms. Scott indicated that the Committee's policy is to refer to PSDQ when changes to scorecard are adopted so that they can figure out an appropriate and statistical relevant way to measure income changes. PSDQ would have to consider missing information, as it's very detrimental to the system and the overall data quality to have missing information. The Continuum worked very hard with all projects to include all information. She expressed that depending on the project type, missing information is generally viewed unfavorably.

Mr. Sullivan noted that not all projects would have the same level of data quality, and that this was being checked by providers. He added that the same percentage of missing information would show up in Annual Performance Reporting **(**APR) and data quality reports. It would be concerning on the data quality section of the scorecard if that much information were missing.

Discussion ensued on the language used on the scorecard. Mr. Sullivan explained that the only APR that maintained was taken out of was transitional housing, which has increased; other APRs have increased or maintained income. Ms. Scott added that the system performance measures are not measuring "maintained", and that there is a shift in HUD priorities, as well as their determination on a functioning system.

Ms. Donley indicated that the idea is to plug in as a placeholder so as to understand this year's baseline. She inquired about the possibility for the Continuum, as it moves into the next NOFA application cycle, to look into a breakout of individuals with disability income and those in PSH, those who have maintained, etc., and to look at reports to establish a threshold that makes sense.

Mr. Bridwell expressed validity to Ms. Donley's proposal, adding that it should be more in terms of length of stay in a project because if it receives zero income individuals, and income changes within six months, it modifies the threshold. He added that as housing retention that idea is good, and that as long as permanent was compared to permanent, it was okay, but if the Continuum were comparing serving chronically homeless to transitional housing, it becomes unfair.

Co-Chair Newsom inquired if there was a motion to approve the scorecard. Mr. Bridwell indicated that perhaps the Board had not had enough discussion to make a decision. He inquired why Board should wait if the report is consistent, if we can measure permanent to permanent and transitional to transitional, and if it's more substantial information on item #3, the Board should make the change on the scorecard. He expressed the Board could not wait on perfection.

Ms. Schwabenlender inquired about whether Mr. Bridwell was suggested that income improvement was added and points were attached, or if it was added to set up baseline. Mr. Bridwell responded that it was added, and that it replaces section 3 with a point value.

Discussion ensued on missing information. Ms. Schwabenlender expressed that if the Continuum indicated if it wanted to add with points, the Board would have to be comfortable with whomever was tasked with doing the work to be calculated and measured similarly across the board. Ms. Scott indicated that PSDQ would have to come up with the mechanism. She added that when the APR is measured, the missing information is counted against the project.

Co-Chair Hartke expressed it would be unfair to ask providers for information that was not previously requested and for which they were unprepared to provide. He continued he was more comfortable with the placeholder since it was difficult to score providers if they hadn't collected information, as opposed to a placeholder to indicate this was now in effect.

Brande Mead, MAG, indicated this report was not one that was previously pulled, but that the data, a performance benchmark that HUD was been requesting, has been collected by providers. She added that the Continuum has changed the local scorecard to include "maintain", while HUD is requesting increases in income.

Discussion ensued regarding language on various reports. Ms. Scott indicated that the Continuum is requesting for all information pertaining to "maintain" or "increase", and that it was adding points for increase in cash benefits and noncash benefits.

Karen Kurtz, CBI, indicated that it's not necessarily that projects haven't had the data, but that in some cases, income data is not updated until income recertification is run, which is done at the end of lease cycles. She expressed that if that change was going to be implemented, it should be done with advance

notice so that operations have the opportunity to change their practices and to update their income more frequently.

Keith Thompson, Phoenix Shanti, requested that if the second group and Housing First were priorities, that it be made clear that drug testing and eviction for alcohol and drug use were not a practice of the project, so that recovery housing, who will not receive those points, will not be penalized. Mr. Bridwell suggested that as a middle ground, the Continuum should take the available points and the existing three, divide them and put the other half into a new category with a new report to reflect the scoring that is taking place.

In response to Mr. Thompson, Ms. Scott indicated that the group that met on Friday discussed the criteria for Housing First, but the group did not come to a consensus. She added that there were lots of existing tools to calculate Housing First, and that Mr. Thompson's concerns were thresholds that are widely believed to be principles within Housing First. She expressed that it was up for consideration on how to define Housing First.

Ms. Kurtz inquired whether recovering housing was being scored equal with Housing First. Ms. Scott responded that it was not, and that Friday's group proposed giving extra points for Housing First. She continued that the question remains on whether Housing First should be more clearly defined, and whether drug testing and eviction based on a positive drug test constitutes a violation of Housing First. Ms. Scott added that while the Continuum went through a process of defining recovery housing, neither the Board nor the Committee adopted any points associated with that for the program performance scorecard. Ms. Scott clarified that the Continuum cannot define recovery housing as Housing First, but that it could decide to weigh it equally.

Mr. Bridwell moved to accept the scorecard with the recommendation that rather than waiting on 0554.01, the Board insert that report and use that as the measurement, as opposed to item #3 of the maintained and increased measurement. Additionally, he suggested that behind the housing first project commitment, there is some sign-on to core values of Housing First principles and that compliance to community adopted standards of excellence agree that there should be no score; however, he stipulated that there should be a formal sign-on to the CoC adopted community standards of excellence, indicated as yes or no. Mr. Bridwell added it would probably be yes by that time. Because there was no second, the motion died.

Ms. Garganta indicated she would like to accept all the changes, with the exception of section #3, and to insert the income change management solely as to establish a baseline and to continue having the three still identified as such, but using the baseline of 0554.01 to establish income level. She added that her motion was as-is, just inserting the baseline and keeping #3 as is, taking the missing information into account. Co-Chair Hartke seconded the motion.

Diana Yazzie-Devine, Native American Connections, expressed concern that recovery housing would score considerably lower, ending up in Tier 2, resulting in all recovering housing monies being lost. She added that by not getting points in the Housing First category, Housing First would automatically score lower, and that up until now, they had been receiving those points.

Ms. Scott explained that there was a Housing First preference in the last scorecard as well, and that recovery housing was at a disadvantage last year. Mr. Gallegos expressed that loss of recovery dollars was very concerning because there is a high need for outreach. Co-Chair Hartke indicated that the goal should be to score as high as possible on HUD's criteria, and that there would be some fallout, but that those shouldn't lower the total funding. He expressed that the Continuum should look at HUD priorities and align those goals for this application to secure as much money as possible. He added that it's not saying those are not priorities, but that was the reason he was in favor of the changes.

Charlene Flaherty, Corporation for Supportive Housing (CSH), clarified that another definition for Housing First cannot be created because a set criteria and standards is already in place, and that although recovery housing was a necessity in the community, it was not Housing First. She pointed out that that Housing First is the priority for the application.

Discussion ensued on recovery housing and Housing First. Mr. Thompson requested that if there was a Housing First priority, that the Continuum be very clear that those programs not evict for drug use and not test for drug use so that those projects that do, have the benefit of the fewer points. He added that if those projects end up on Tier 2, so be it.

Mr. Bridwell agreed, adding that projects that identify as Housing First really do need to be Housing First projects.

Co-Chair Newsom called for a vote on the motion to pass as-is. The motion passed unanimously.

Ms. Scott indicated it may be appropriate to have two motions to determine the following: to define Housing First, and to ask all the providers to run their scorecard and to return to the CoC within a week so the Board may have an opportunity to review them as a self-score.

Co-Chair Hartke added that this was a preliminary report for an idea on where things are, and to help providers to score higher. Co-Chair Newsom requested feedback on the week timeline, and Ms. Lord expressed it as not enough time, especially since many providers were going to attend the National Endowment for Humanities (NEH) conference the following week.

Discussion ensued on a feasible timeframe for feedback. Ms. Donley added that the strategic discussion looked at suggestions on how to approach Tier 1 and Tier 2: does the Continuum use the same approach as last year? Should it use HUD's approach by recommending a Tier 1 and Tier 2 that matches its priorities? She proposed having a draft scorecard as a strategic conversation before the ranking and review process.

Mr. Bridwell indicated that because the Continuum is not likely to score higher than last year, it is anticipating another loss of funding with $1.7 million in Tier 2. He added that the CoC could be more strategic in Tier 1 to have a better outcome in Tier 2, and that it should work with providers to make adjustments to better protect what ends up in Tier 2.

Ms. Scott indicated that a discussion was to have a preliminary scorecard; the cost effectiveness formula will be included, which is the top 25 percent of those rated. In terms of CoC funds, the cost per positive housing outcome would get 5 points; the middle would get three points and the bottom would zero points. Ms. Scott expressed that with the exception of coordinated entry, everything had been decided to date on a one-year timeframe. She pointed out that the CoC was now eight weeks away from having material due to HUD, and that if projects could give a cost per positive housing outcome, the positive housing outcomes can be defined in the APR. The Continuum will be measured to the degree that it reallocates funding in the 2016 NOFA, which will factor into the overall Continuum score.

Mr. Bridwell indicated he views it as a self-score, the only one that would need guidance was when the score was against the Continuum. He suggested having an average cost for a particular category, the idea was to group the providers that the Continuum needed to talk to and help. He added that just like the Continuum wasn't going to change its score too much, it was just as unlikely that the providers would change their score much in a very short time span. He suggested that if it was easier, the Board could do all the same, knowing it is doing the same analysis as last year.

Ms. Yazzie-Devine raised concern about using last year as a guideline, but that this issue could be discussed at the next Board meeting.

Ms. Mead inquired about the Board's desire to have a strategic planning session based on preliminary data, which was scheduled for August 8th. Ms. Garganta indicated it was her preference to use last year's data and for organizations to self-score and be truthful in their areas of strengths and weaknesses, thereby creating their own baseline.

Discussion ensued on self-scoring. Ms. Yazzie-Devine suggested that self-scoring is a common practice, and that it should be voluntary. Mr. Liggett agreed it might make sense.

Jacki Taylor, Save the Family, expressed that providers weren't saying they weren't open to scoring; she indicated that it is critical for the CoC to have a clear definition of how the points are calculated.

Mr. Bridwell suggested that the sheet be reformatted so that the projects that are no longer funded by the Continuum are brought down below. This way, it would be easier to see what projects the CoC is dealing with.

Co-Chair Newsom moved onto #9, System Performance Measures.

9. System Performance Measures

Co-Chair Newsom invited Margaret Kilman, MCHSD, a member from PSDQ, to provide an update on the region's systems performance measures. Ms. Kilman indicated that the systems performance measures were developed by HUD to help establish national benchmarks and targets. Additionally, local communities would also be able to use these to establish CoC goals. HUD would also use this data to see how CoCs are aligning with HUD policy priorities. Some of the local criteria that HUD has suggested that communities consider are the following: demographics that make up our population, specifically the target populations that HUD has given guidance on; local priorities; ensuring the CoC is as strategic as possible; targeting subpopulations, and how the CoC is performing ending chronic homelessness. Ms. Kilman indicated that these measures would also be used for the NOFA, and that much of what was discussed today can help with resource allocation, aligning with HUD policy priority and regional planning.

She continued that HUD has provided a lot of guidance for these system performance measures, which will help focus on common measures, and assist in measuring the collective impact of program and system goals. She expressed that HUD was moving away from one project individually, but was looking more at the following: how projects impact the system of care; measuring the CoC's track on ending homelessness; increased performance in the CoC application; accountability for system and projects within the system, and systems response (how systems are integrated).

The first measure, length of time homeless, measures how long a person experiences homelessness. The outcome that HUD measures is the reduction in the average and median length of homelessness a family or individual experiences. Ms. Kilman presented data submitted by CIR with an average length of homeless as 58 days, and a median length of homeless as 30 days. The overall community performance within six month is 7.8 percent return to homelessness rate; in the 6-12 month range: a five percent return to homeless rate; in the 13-24 month range: 5.3 percent return to homeless rate, and for greater than 24 months, an 18 percent return to homeless rate was reported. Ms. Kilman indicated that the actual measures have the breakouts.

The number of homeless persons in the community and in the CoC (measure #3) is broken down into two sections: sheltered and unsheltered persons in the point in time (PIT) count, and

all persons in emergency shelter, safe haven and transitional housing during the year. The change reported in the PIT is a five percent decrease, with 14,458 as a reported amount of unduplicated number of persons served in emergency shelter and safe haven. Last year, it was 15,167.

The employment and income change (measure #4) measures all "stayers" and "leavers" with an annual assessment for those who have increased their employment. There are six sub-measures; four of which measure change in total income for all stayers and leavers throughout the CoC. HUD's objective is to increase the households that gain or increase income in the reporting period.

The "first time homeless" measure is measured by the number of persons who enter emergency shelter, safe haven or transitional housing during the reporting period for the last year and the current year, resulting in the difference in the end. This measure also indicates entries would be considered "new" if entered within that timeframe, and that the CoC's goal is to reduce the number of individuals who become homeless for the first time, resulting in a reduced number of first-time entries within 24 months in HMIS year over year. The measure also looks at the change in the number of individuals entering emergency shelter, safe haven, transitional housing, permanent housing and permanent housing projects. Ms. Kilman indicated that the workgroup has debated on how to look at projects within the system; how system performance measures are related to each other; what the highest impact changes are when looking at data collectively. Taken as a whole, these indicators will help the Continuum have an indicator of where it should be.

"Homelessness prevention" (measure #6) also measures housing placement. Currently, no prevention services are funded, so no data has been reported.

"Successful housing placement" (measure #7) looks at the number of people who engage in emergency shelter, safe haven, transitional or street outreach that were able to move on to a permanent housing placement. Ms. Kilman indicated that there is an increase in the number of people exiting street outreach, emergency shelter, transitional housing and permanent housing. They are exiting and maintaining permanent housing. The goal is to have successful housing placements, which include the number from street outreach and emergency shelter.
The street outreach looks at whether people are exiting into emergency shelter, while everything else looks at positive housing outcomes.

Ms. Kilman indicated that after looking at these measures for the last several months, it raises questions such as, what other data the CoC should be looking at, and where it should be asking other questions.

Discussion ensued on whether people avoid homelessness due to homeless prevention service or intervention. There were no other comments.

10. Report on the Closure of the Overflow Beds at the Human Services Campus
Co-Chair Newsom invited Mr. Liggett to present information. He indicated that the overall project is coordinated by the funder's collaborative in terms of what the Campus has been doing with the overflow shelter. The previous overflow arrangement was in operation since the MOS and parking lot closed. He added that the parking lot was an open lot and the building used for overflow was deemed unsafe, while the parking lot was regarded as inhumane. The Funder's Collaborative began preparing for an alternative model in November, 2014. Mr. Liggett continued that the group worked with Lodestar Day Resource Center (LDRC) and St. Vincent de Paul, who have done a great job operating a humane environment that is professionally staffed without the need for police presence, where clean sheets and mattresses are provided on a nightly basis. While the model is temporary, it has been successful and has been working well. Mr. Liggett indicated that the overflow has not been phased out and that money has not been cut. Further, he estimates that since planning commenced for housing placements, while making housing placements and the new model (which will be phased out by this fall), an additional $4.4 million were brought into the system, on top of what was being used for the overflow. With the new temporary arrangement, the model began with 430 people a night; 14 months later, it is down by 111 people. Mr. Liggett explained that the trend is in the right direction, and that in the 14 months, almost 7,000 people have used the service. Money is being redirected to housing first as a priority. Phasing out will begin with three different groups at the overflow campus:

- People sleeping outside the campus by their own choice;
- Single men (the next largest group) and finally,
- Women and men with disabilities, which will be the last group to go in October.

Mr. Liggett expressed that efforts are ongoing, and that the group is considering expanding other shelter options for that time period, as there will still be individuals needing service.

10. Request for Future Agenda Items
There were no additional items requested.

11. Comments from the Board
There were no further comments.

Adjourn
The meeting was adjourned by Co-Chair Newsom at 4:10 pm. The next Board meeting is scheduled for August 29, 2016.

Prioritization Recommended by HUD

Re. HUD Notice CPD-16-11, issued July 25, 2016

Notice on Prioritizing Persons Experiencing Chronic Homelessness and Other Vulnerable Homeless Persons in Permanent Supportive Housing

"HUD encourages all CoCs adopt into their written standards the following orders of priority for all CoC Program-funded PSH. CoCs that adopted the orders of priority established in Notice CPD-14-012, which this Notice supersedes, and who received points for having done so in the most recent CoC Program Competition are strongly encouraged to update their written standards to reflect the updates to the orders of priority as established in this Notice. Where a CoC has chosen to not incorporate HUD's recommended orders of priority into their written standards, recipients of CoC Program-funded PSH are encouraged to follow these standards for selecting participants into their programs as long as it is not inconsistent with the CoC's written standards."

Dedication and Prioritization of Permanent Supportive Housing Strategies to Increase Number of PSH Beds Available for Chronically Homeless Persons

A. **Increase the number of CoC Program-funded PSH beds that are dedicated to persons experiencing chronic homelessness.**
B. **Prioritize non-dedicated PSH beds for use by persons experiencing chronic homelessness.**

Order of Priority in CoC Program-funded Permanent Supportive Housing

A. **Prioritizing Chronically Homeless Persons in CoC Program-funded Permanent Supportive Housing Beds *Dedicated or Prioritized* for Occupancy by Persons Experiencing Chronic Homelessness**
   1. CoCs are strongly encouraged to revise their written standards to include an order of priority, determined by the CoC, for CoC Program-funded PSH that is dedicated or prioritized for persons experiencing chronic homelessness that is based on the length of time in which an individual or family has resided in a place not meant for human habitation, a safe haven, or an emergency shelter and the severity of the individual's or family's service needs. Recipients of CoC Program-funded PSH that is dedicated or prioritized for persons experiencing chronic homelessness would be required to follow that order of priority when selecting participants for housing, in a manner consistent with their current grant agreement.
   2. Where there are no chronically homeless individuals and families within the CoC's geographic area, CoCs and recipients of CoC Program-funded PSH are encouraged to follow the order of priority in Section III.B. of this Notice. For projects located in CoC's where a sub-CoC approach to housing and service delivery has been implemented, which may also be reflected in a sub-CoC coordinated entry process, need only to prioritize assistance within their specified sub-CoC area. 2
   3. Recipients of CoC Program-funded PSH should follow the order of priority above while also considering the goals and any identified target populations served by the project. For example, a CoC Program-funded PSH project that is permitted to target homeless persons with a serious mental illness should follow the order of priority under Section III.A.1. of this Notice to the extent in which persons with serious mental illness meet the criteria. In this example, if there were no persons with a serious mental illness that also met the criteria of

chronically homeless within the CoC's geographic area, the recipient should follow the order of priority under Section III.B for persons with a serious mental illness.

4. Recipients must exercise due diligence when conducting outreach and assessment to ensure that chronically homeless individuals and families are prioritized for assistance based on their total length of time homeless and/or the severity of their needs. HUD recognizes that some persons–particularly those living on the streets or in places not meant for human habitation–might require significant engagement and contacts prior to their entering housing and recipients of CoC Program-funded PSH are not required to allow units to remain vacant indefinitely while waiting for an identified chronically homeless person to accept an offer of PSH. CoC Program-funded PSH providers are encouraged to follow a Housing First approach to the maximum extent practicable. Therefore, a person experiencing chronic homelessness should not be forced to refuse an offer of PSH if they do not want to participate in the project's services, nor should a PSH project have eligibility criteria or preconditions to entry that systematically exclude those with severe service needs. Street outreach providers should continue to make attempts to engage those persons that have been resistant to accepting an offer of PSH and where the CoC has adopted these orders of priority into their written standards, these chronically homeless persons must continue to be prioritized for PSH until they are housed.

B. Prioritizing Chronically Homeless Persons in CoC Program-funded Permanent Supportive Housing Beds *Not Dedicated or Not Prioritized* for Occupancy by Persons Experiencing Chronic Homelessness

(a) **First Priority–Homeless Individuals and Families with a Disability with Long Periods of Episodic Homelessness and Severe Service Needs**

An individual or family that is eligible for CoC Program-funded PSH who has experienced fewer than four occasions where they have been living or residing in a place not meant for human habitation, a safe haven, or in an emergency shelter but where the cumulative time homeless is at least 12 months **and** has been identified as having severe service needs.

(a) **Second Priority–Homeless Individuals and Families with a Disability with Severe Service Needs.**

An individual or family that is eligible for CoC Program-funded PSH who is residing in a place not meant for human habitation, a safe haven, or in an emergency shelter and has been identified as having severe service needs. The length of time in which households have been homeless should also be considered when prioritizing households that meet this order of priority, but there is not a minimum length of time required.

(b) **Third Priority—Homeless Individuals and Families with a Disability Coming from Places Not Meant for Human Habitation, Safe Haven, or Emergency Shelter Without Severe Service Needs.**

An individual or family that is eligible for CoC Program-funded PSH who is residing in a place not meant for human habitation, a safe haven, or an emergency shelter where the individual or family has not been identified as having severe service needs. The length of time in which households have been homeless should be

considered when prioritizing households that meet this order of priority, but there is not a minimum length of time required.

(c) **Fourth Priority–Homeless Individuals and Families with a Disability Coming from Transitional Housing.**

An individual or family that is eligible for CoC Program-funded PSH who is currently residing in a transitional housing project, where prior to residing in the transitional housing had lived in a place not meant for human habitation, in an emergency shelter, or safe haven. This priority also includes individuals and families residing in transitional housing who were fleeing or attempting to flee domestic violence, dating violence, sexual assault, or stalking and prior to residing in that transitional housing project even if they did not live in a place not meant for human habitation, an emergency shelter, or a safe haven prior to entry in the transitional housing.

Maricopa HMIS
Policies and Procedures

Table of Contents

Vision Statement 1
Introduction 1
HMIS ..... **Error! Bookmark not defined.**3
Terminology 4
Roles and Responsibilities 7
HMIS Lead Agency and System Administrator 7
HMIS Management 7
HMIS Documentation ..... **Error! Bookmark not defined.**
Participating Agency 10
Executive Director 12
Agency Administrator 13
User 15
Clients 18
Communication 20
From HMIS Lead Agency and System Administrator 20
To HMIS Lead Agency and System Administrator 20
Maricopa HMIS Help Desk 21
Access 21
HMIS Lead Agency and System Administrator ..... **Error! Bookmark not defined.**21
Security 23
HMIS Software Vendor ..... **Error! Bookmark not defined.**24
Licensed Users 26
Location of Data Access 28
Agency Data 29
HMIS Data Sharing 30

Visibility Settings 32
Client Denial to Share 32
Data Shared Information 33
Data Quality 33
Licensing and Invoicing 34
Grievances 34
From a Participating Agency or Client to the Maricopa HMIS 34
Participation Termination 35
Initiated by the Participating Agency 35
Initiated by HMIS Lead Agency and System Administrator 35
Projects in HMIS 36
Adding a New Project in Maricopa County by Participating Agency 36
Making Changes to Existing Projects in HMIS 36
Additional Customization 37
Acknowledgement of Receipt of the HMIS Policies and Procedures Manual 38
ATTACHMENT A Maricopa HMIS Partnership Agreement 39
ATTACHMENT B Code of Ethics 50
ATTACHMENT C Release of Information 52
ATTACHMENT D Software Vendor Security Plan 54
ATTACHMENT E Maricopa HMIS Data Quality Plan 64
ATTACHMENT F Maricopa HMIS Privacy Notice 75
ATTACHMENT G Maricopa Security Plan 83
ATTACHMENT H Report Request Form 94
ATTACHMENT I Report Update Form 96
ATTACHMENT J New Project/Project Update Form 98

Vision Statement

The Homeless Management Information System Project (HMIS) produces timely, accurate, and complete information for stakeholders working to end homelessness in Maricopa County.

Background

The 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 Community Information and Referral Services (CIR) 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 and Referral Services is the HMIS Lead Agency and System Administrator for implementation of the HMIS project. 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 CIR enters into negotiations with Bowman for ServicePoint, and contract for co-location of the servers and database with Bowman.

Introduction

The Maricopa County Homeless Management Information System (HMIS) was developed to support the Maricopa County homeless providers and partner with agencies in their missions, by supplying them with the tools to meet the reporting requirements for their projects. The HMIS provides information to the U.S. Department of Housing and Urban Development (HUD), local nonprofits, state-level policy makers, federal partners and other advocates in the mission to end homelessness.

The HMIS is a client information database that provides a standardized assessment of client needs, creates individualized service plans, and records the use of housing and services. The fundamental goal of the HMIS is to use the data to determine the utilization of services of participating agencies, identify gaps in the local service continuum and develop outcome measurements, according to the HUD/Maricopa County CoC HMIS standards. The HMIS can identify patterns in the utilization of assistance, as well as document the effectiveness of services for clients.

All this will be accomplished through data analysis of the actual experiences of persons experiencing homelessness, as well as the service providers who assist them in shelters and homeless assistance projects throughout the state. This data may also be analyzed to provide unduplicated counts and anonymous aggregate data to policy makers, service providers, advocates and consumer representatives. Statewide reporting is based on aggregate, non-identifying data; therefore, such data may be shared with the public without specific permission.

The HMIS uses a web-based software project from the HMIS Software Vendor called ServicePoint, which resides on a central server to facilitate data collection by homeless service organizations in Maricopa County. Access to the HMIS is limited to agencies and authorized staff members who have met the necessary training requirements and have signed the necessary privacy, data sharing (if applicable), security and licensing documentation (if applicable), as listed in this manual. As the guardians entrusted with personal data, agencies have both a moral and a legal obligation to ensure that data is being collected, accessed and used appropriately. All agencies must be vigilant to maintain client confidentiality, treating the personal data of Arizona's most vulnerable populations with respect.

Every Maricopa project that receives federal homeless project funds from HUD is required to enter data on persons served with those funds into the HMIS. Some projects funded through the U.S. Veterans Administration and the U.S. Department of Health and Human Services may be required to enter data into the HMIS, as well. In addition, the HMIS encourages agencies that do not receive federal funds to participate in the HMIS so that service provision in the Maricopa Regional Continuum of Care is coordinated and that data represents the broader network of service provision in the continuum.

The data standards also require organizations to comply with any federal, state and local laws that require additional confidentiality protections, including but not limited to:

- The Health Insurance Portability and Accountability Act of 1996 (45 CFR Parts 160 and 164);
- The Confidentiality of Alcohol and Drug Abuse Patient Records Rule (42 C.F.R. Part 2);
- The Violence Against Women Act (VAWA).

As these data standards are subject to change, all providers are responsible for monitoring for updates and being in constant compliance with all data standards.

HMIS

Community Information and Referral Services (CIR) is the lead agency for the HMIS implementation in the Maricopa County Regional Continuum of Care (AZ-502).

To ensure the integrity and security of sensitive client confidential information and other data maintained in the database, CIR requires all participating agencies to sign the HMIS Partnership Agreement (Attachment A). All end users must sign a Code of Ethics Agreement (Attachment B) prior to being given access to the HMIS. All clients must sign a Release of Information (Attachment C) prior to entry of the individual's data into the system.

Terminology

Many of the terms used in the HMIS Policies and Procedures Manual may be new to many readers. It is important to understand the terms used to better understand the roles, responsibilities and liabilities of the HMIS.

Advanced Reporting Tool (ART): HMIS Software Vendor partners with S.A.P. Business Objects to give users access to a wide variety of reports. The ART is used commonly for federal reporting and project customization of reports.

Agency Administrator: The person responsible for HMIS administration at the participating agency level and is the lead agency contact with CIR.

Annual Homeless Assessment Report (AHAR): The report to the U.S. Congress on the extent and nature of homelessness in America.

Annual Performance Report (APR): The HUD-required report used to track progress and accomplishments of COC-funded projects.

Maricopa County Regional Continuum of Care: The HUD recognized Continuum of Care comprised of homeless programs in Maricopa County, Arizona.

Maricopa County Homeless Management Information System (HMIS): The database used collectively by partnering agencies within the Maricopa Regional Continuum of Care to track client service records, coordinated assessment, service needs, progress and accomplishments of clients served.

Maricopa Association of Governments (MAG): The CoC lead entity for the Maricopa Regional Continuum of Care.

Authentication: The process of identifying a user to grant access to a system or resource based on a username and password.

Client: An individual who has inquired, is receiving, or has received, *services* from a participating HMIS project that collects or maintains personally-identifiable service information.

Client Acknowledgement Form: The form signed by clients authorizing or denying their client specific information be collected and shared via the HMIS project.

Code of Ethics Agreement: An agreement between participating agency users and CIR that allows access to HMIS.

Continuum of Care (COC) Project: Project receiving funding from HUD through the competitive COC application process. These projects are identified in the HMIS as COC projects.

Executive Director: A person who serves as the top executive official of a participating agency. This person may have a title of chief executive officer or president, etc.

HMIS Software Vendor: The company/vendor responsible for the HMIS software. Bowman holds the contract for HMIS and ServicePoint under a contract with Community Information and Referral renewed annually with the last renewal executed in November 2015.

HMIS Lead Agency and System Administrator (LASA): Completes the functions of the administrating the HMIS software. Community Information and Referral is the Lead Agency and System Administrator (LASA) for the HMIS under a Memorandum of Understanding between Community Information and Referral and the Maricopa Association of Governments Regional Continuum of Care executed in May 2016.

Housing Inventory Count (HIC): The inventory of beds for persons experiencing homelessness, including seasonal and overflow beds.

Participating Agency: Any agency/project that enters client-level information into the HMIS.

Point In Time (PIT): The annual **count** of sheltered and unsheltered persons experiencing homelessness on a single night.

Release of Information (ROI): A statement signed by the client authorizing or denying the participating HMIS agency/project to give other participating agencies their personal information and information regarding the client's situation.

ServicePoint: A software package written by HMIS Software Vendor, which tracks data about people in housing crisis to determine individual needs, provide a referral system and create aggregate data for reporting and planning. The software is web-based and uses a standard graphical user interface similar to Microsoft Windows.

User: An individual who has been granted access and uses HMIS. Users are the main guardians against violating a person's confidentiality.

Roles and Responsibilities

Community Information and Referral Services (CIR)

CIR is the lead agency for the implementation and maintenance of the HMIS.

CIR HMIS Management

Policy: CIR as the System Administrator and HMIS Lead Agency is responsible for the organization and management of the HMIS. CIR is responsible for all system-wide policies, procedures, communication and coordination of the HMIS.

Procedure: CIR will follow protocols established by HMIS Software Vendor, LLC, in regard to unauthorized access, as established on pages nine (9) and ten (10) of the HMIS Software Vendor Securing Client Data Policy Manual. An HMIS team member will notify HMIS Software Vendor of any software issues within twelve (12) hours of being made aware of the issue and an investigation at the System Administrative level has taken place. All information received from HMIS Software Vendor pertaining to use, access, reporting or live site system will be disseminated to Executive Directors or his/her designee within three (3) business days of receipt. No user, Executive Director or agency may contact Bowman System directly, without the express written consent of CIR. The HMIS Lead Agency/System Administer will contact Bowman System to coordinate system updates, software issues and other system administration functions.

HMIS Documentation

This document includes the HMIS Policies and Procedures Manual, the HMIS Data Quality Plan, the Maricopa County Security and Privacy Plan, the HMIS Code of Ethics Agreement, the HMIS Partnership Agreement, the Client Acknowledgement Form and all other related forms.

Policy: LASA will provide the necessary manuals and forms for all users. These documents will be kept up-to-date and in compliance with all HUD policies and requirements. Agency Administrators will be responsible for downloading and distributing to end users within the agency the HUD Data Standards Manual available on LASA website www.211arizona.org/HMIS or the HUD Exchange website https://www.hudexchange.info/.

Procedure: LASA will review the HMIS Policies and Procedures Manual, the Data Quality Plan, the Security and Privacy Plan, the Code of Ethics Agreement, the Partnership Agreement, the

Client Acknowledgement Form, the Agency Update Form and related forms annually and they will be updated based on HUD regulatory changes and requirements.

Agencies must submit an updated Agency Update Form when changes occur in the programs that necessitate updating. The beginning of each calendar year, the documents will be reviewed and updated. In the event HUD issues interim changes to the requirements, affected policies and procedures and any related documentation will be reviewed and updated at that time, as well. All changes will be communicated to participating agencies through the Maricopa HMIS Committee meetings, HMIS system (i.e., "System News") and electronically through the end user e-mail distribution list. All documents will be available for download at www.211arizona.org/hmis.

Security Management

Policy: LASA will be responsible for the continuous monitoring of security and user access.

Procedure: Refer to HMIS Software Vendor Securing Client Data Policy Manual (Attachment D).

Training

Policy: LASA will provide timely training for all new users, continuing education and ART reporting in the most efficient and effective way possible.

Procedure: LASA will provide training to all users through the HMIS Training Academy offering online and in person trainings. LASA will also notify participating agencies and users of upcoming trainings through the System News available in ServicePoint and/or electronically. Agencies will be given no less than thirty (30) days advance notification of in person trainings on the calendar. LASA will conduct all new user training, specialized training relevant to user position and report training. At no time will a participating agency contact Bowman directly for training. The System Administrator will send training confirmation responses to registered users within three (3) business days of online registration.

Agency Management

Policy: LASA will set-up and terminate agencies, projects and users, as needed.

Procedure: Agencies will notify LASA of new projects and new users electronically or by telephone by contacting LASA HMIS Help Desk at HMISsupport@cir.org or (602) 908-3605.

User Management

Policy: LASA will give appropriate levels of access to the system based on user's position in the participating agency, configuration of projects and designation by the Executive Director.

Procedure: LASA in consultation with the participating agency Executive Director or his/her designee will assign appropriate user levels when adding a new user. LASA will always assign the most restrictive access to users while still allowing efficient job performance to protect client confidentiality or privacy.

System Availability

Policy: HMIS Software Vendor will provide a highly available HMIS and will inform users in advance of any planned interruption in service.

Procedure: Scheduled upgrades and maintenance will occur on Friday nights after 9:00 p.m. MST. LASA will inform users of the exact date and time at least three (3) business days prior to scheduled upgrade via ServicePoint System News and direct e-mail to all end users on record. In the event of an unscheduled unavailability, LASA will contact the end users via email and inform them of the cause and the anticipated duration of the interruption of service. Users will be notified as quickly as possible of system unavailability, but in no case more than twenty-four (24) hours after service interruption.

Participating Agency

A participating agency is one that enters client-level data into the HMIS.

Security Management

Policy: Agencies are responsible for ensuring all hardware and software used to access and/or store HMIS client-level data is in a secure location where access is restricted to authorized staff. Agencies must comply with the Maricopa HMIS Security and Privacy Plan.

Procedure: Agencies may be monitored for security by LASA through remote or on-site compliance visits. Failure to comply will result in deactivation of all agency user accounts and the agency may be non-compliant with HUD and/or other funding regulations.

Records Management

Policy: The participating agency must maintain appropriate documentation of any client Release of Information and Client Acknowledgement Form records obtained in a secure location for a period of five (5) years after the last date of client service and assure their subsequent destruction by shredding. In addition, agencies must keep Agency Update Forms, Agency Partnership Agreements, Data Sharing Agreements, Opt-out Requests, grievance documentation and all other HMIS related documentation in a secure location for a period of five (5) years.

Procedure: Records must be made available to the client, upon written request, within fourteen (14) business days. Compliance monitoring is completed by LASA, as requested by funders or required by regulation. Agencies will be required to show proof of compliance with the above policy at time of compliance monitoring. Failure to comply will result in deactivation of all agency user accounts and the agency may be non-compliant with HUD and/or other funding regulations.

Privacy Management

Policy: Agencies will be solely responsible for ensuring clients understand privacy. With the exception of agencies providing services solely to children and youth, all agencies must obtain a signed Client Acknowledgement Form from each client before entering data into the HMIS. Clients in Runaway and Homeless Youth (RHY) Programs and private programs that serve only children and youth will NOT be asked to provide a Client Acknowledgement Form. All HMIS agencies must post a Privacy Notice at all intake

locations. A copy of the Privacy Notice will be made available to all clients at the client's request.

Procedure: A copy of the Privacy Notice and the current Client Acknowledgement Form can be found at www.211Arizona.org/HMIS. Clients may request to not share their data in the HMIS. In that case, clients would be entered by locking the record. Records may be locked by contacting the LASA. The Client Acknowledgement Form will be in effect for one (1) year from the date of signing. Upon Recertification of client, new Client Acknowledgement Form must be signed for all programs except those serving solely children and youth.

HMIS compliance monitoring when needed or required will be completed by the LASA as the System Administrator for HMIS. Agencies will be required to show proof of compliance with the above policy at time of compliance monitoring. Failure to comply will result in deactivation of all agency user accounts and the agency may be non-compliant with HUD and/or other funding regulations.

Data Sharing

Policy: Data sharing of the HUD Universal Data Elements among participating HMIS agencies began in 2013. Agencies can share with other agencies with a signed MOU or Data Sharing Agreement indicating a desire to share data. All HOPWA projects are currently prohibited from participation in data sharing. All other data sharing policies and agreements will be noted in the Maricopa HMIS Data Sharing Policy.

Procedure: All projects, with exception of HOPWA and RHY will have the opportunity to share client-level data. The continuum wide client-level data sharing privileges in HMIS is currently the HUD Universal Data Elements (UDEs) only. Participating agencies have the opportunity to sign a Data Sharing Agreement or MOU with other agencies. All agreements need to detail items to be shared and signed by all parties. Verbal agreements are not acceptable. Agencies will comply with the Maricopa County Data Sharing Policy.

Executive Director

The Executive Director or designee is responsible for ensuring their agency and all licensed users within their agency abide by all COC established regulations, standards, policies and procedures in regards to the HMIS and clients' rights.

Documentation

Policy: Before any agency user is given access to the HMIS, the Executive Director or his/her designee must complete and submit the necessary original documentation to LASA to keep on file.

Procedure: The Executive Director or his/her designee **must** read, understand, and sign the HMIS Partnership Agreement bi-annually (50% of agencies each year). Read, understand, and sign each of the agency's users' HMIS Code of Ethics Agreements annually. Update the Agency Update annually when necessary.

In addition, the Executive Director must comply with approved Maricopa HMIS User Frees annually for HMIS participation. Invoices will be sent to all agencies during the first quarter each fiscal year. Failure to comply with payment of User Fees within 90 days of invoice will result in deactivation of all agency user accounts, unless CIR as the System Administrator is made aware and agrees to extenuating circumstances/payment plan option.

Ultimately Responsible

Policy: The Executive Director or his/her designee is the person ultimately responsible for compliance with all policies and procedures in this manual; which includes but is not limited to: knowledge and understanding of client rights, grievance procedures, data sharing, agencies security and all actions and work conducted by licensed users in their agency, including those no longer employed at their agency.

Procedure: The Executive Director must verify and sign all reports or information distributed by their agency for submission or publications. The Executive Director or his/her designee must notify LASA within twenty-four (24) hours if a user should be removed from the HMIS by calling the LASA HMIS Help Desk at (602) 908-3605 or at HMISsupport@CIR.org.

The Executive Director is responsible for ensuring that all their agency HMIS users comply with the Code of Ethics agreement. Agencies with users who fail to comply with the Code of Ethics agreement may be suspended from the HMIS. Failure to comply may result in deactivation of all agency user accounts and the agency may be non-compliant with HUD and/or other funding regulations.

Agency Administrator

An Agency Administrator is the liaison between LASA all agency users. Agency Administrators will be given the role of "Agency Administrator" in the HMIS.

All Agency Administrators must have an e-mail address that is valid and up-to-date and act as the single point of communication between LASA and all of their agency users.

System Management

Policy: Agency Administrators will assist, as needed, the LASA in report development and testing custom reports requested by the agency. Agency Administrators will also be responsible for disseminating all information to users within their agency.

Procedure: Agency Administrators will be made aware via e-mail from LASA of all upcoming system and reporting changes. Agency Administrators are required to test and comment on all custom reports requested by the agency to the HMIS Help Desk at HMISsupport@CIR.org.

If a response from the Agency Administrator is needed, LASA will provide a deadline date for response, which will be no less than five (5) business days and no more than twenty (20) business days. The System Administrator will make the Agency Administrators aware when the final changes are implemented in the HMIS or ART reporting software. Agency Administrators will disseminate system and reporting changes to all other users within their agency within three (3) business days of final change.

When requesting a custom report agencies are required to submit a (Attachments H & I) or a report update form to LASA. These forms will then be reviewed by the LASA HMIS team for approval. If approved, the agency will then receive an estimated development time based on the complexity of the report. The agency might be asked to assist with the report development and validation process. The final report will not be released to the CoC until it has been fully tested by the LASA HMIS team and requesting agency.

When a report is requested by a group of agencies or initiative, meetings will be held during the report request process, development process, and validation process. All

parties will be represented at the meetings to ensure that the needs of all agencies/initiatives are being represented in the custom report.

Agency Management

Policy: The Agency Administrator(s) will be the sole user(s) able and responsible for updating, correcting and maintaining the provider information in the HMIS.

Procedure: Agency Administrators will have the privileges in the HMIS to change and update information regarding their agency and all projects for their agency. Agency Administrators will verify this information quarterly and make changes as necessary. Failure to comply by maintaining correct agency and project information in the HMIS may result in suspension of all agency licenses until corrections are made.

Training

Policy: Agency Administrators have been selected by the Executive Director or his/her designee as the staff member with the skills beyond that of a basic user. Agency Administrators will be required to attend a separate training at least one (1) time per year (twelve (12) months) or as needed/requested by LASA.

Procedure: One (1) hour trainings will be scheduled throughout the calendar year by LASA as the System Administrator for Agency Administrators. The System Administrator may select topics in consultation with LASA and/or based on evaluation of the HMIS FAQs on the Help Desk. Users are responsible for checking dates, times and class agendas on the System News in ServicePoint. Failure to comply with continuing education of the HMIS may result in suspension of the user's Agency Administrator status until requirements have been fulfilled.

User

A licensed HMIS user is responsible for ensuring their agency's client-level data is entered correctly and complies with all client rights, confidentiality and data sharing in compliance with COC regulations, standards, policies and procedures. Users will be assigned an appropriate user role in the HMIS.

Client-Level Data

Policy: Users will not knowingly enter false or misleading information under any circumstances into HMIS regarding the agency, project, or client.

Procedure: Users will submit all reports and/or information to the Agency Administrator/Executive Director for verification prior to submission to LASA. LASA will analyze and verify all data contained in reports and/or information prior to final submission and/or publication. If issues concerning client-level data are raised, LASA may conduct an audit and complete a monitoring site visit. Failure of an agency or user to comply or proof of violation can result in deactivation of the user's license permanently.

Ethical Data Use

Policy: Data contained in the HMIS will only be used to support the delivery of homeless and housing services. Each HMIS licensed user will affirm the principles of ethical data use and client confidentiality contained in the HMIS Policies and Procedures Manual and the HMIS Code of Ethics Form.

Procedure: Users will sign a HMIS Code of Ethics Form and receive user training before being given access to the HMIS. Any individual or participating agency misusing, or attempting to misuse, the HMIS will be denied access. Without limitation the failure to comply with the policies and procedures related to the HMIS, may subject the agency to discipline and termination of access to the HMIS.

Data Sharing

Policy: At no time shall a licensed user alter, change or delete other agency's data when participating in data sharing agreements.

Procedure: If at any time, client data is in question/conflicting, the HMIS users **must**: 1) contact his/her own Agency Administrator and explain the data in question; and 2) either contact the agency that originally entered the data to receive clarification or ask the Agency Administrator to contact the agency that originally entered the data. If a resolution or conclusion cannot be reached between the users, the Executive Directors or designees of concerned agencies must come to a resolution regarding correct data entry. At any time, LASA can be requested, in written form, to analyze audit trails for investigative purposes. If a resolution cannot be determined by the Executive Directors or designees of both agencies, one will be determined by LASA.

Client Release of Information

Policy: Users are the first to safeguard client privacy through compliance with client confidentiality and data sharing policies.

Procedure: Users in all agencies with the exception of those that provide services to Runaway and Homeless Youth (RHY) must obtain a signed Client Acknowledgement Form for each client prior to entering data into HMIS. This can be a release or denial of sharing. If a client denies sharing, the user **must** contact LASA as the System Administrator prior to entering client-level data into the HMIS. The Client Acknowledgement Form is in effect for one (1) year from the date of signing. If the Client Acknowledgement has expired, the user **must** obtain a new release prior to updating records. Signed Client Acknowledgment forms **must** be secure and retained for five (5) years by the participating agency from the date of the last service for the client.

Initial Training

Policy: All new users must have training with the LASA before entering data into HMIS. LASA and the agency requesting new user access will determine training date(s) within forty-eight (48) hours of user request for access to the system. Training must be completed within thirty (30) days of requesting HMIS user status.

Procedure: The LASA HMIS Training Academy is available for online and in person training. Online training is always available and accessible through the HMIS website

www.211arizona.org/HMIS. In person training will be conducted each month of the calendar year. Users must attend at least one (1) training prior to completing assigned tasks for course completion. If the user is unable to attend an in person training, a twenty-four (24) hour notice **must** be given to LASA. LASA shall provide at least thirty (30) days advance notice of training opportunities.

Continued Education Training

Policy: Users must attend at least one (1) HMIS Refresher Training course every year (twelve (12) months) to maintain the continuing skill set for data collection and reporting.

Procedure: LASA will schedule training options monthly throughout the year and publish information on the System News, monthly HMIS Committee meetings, as well as send notices directly to users. LASA as the System Administrator shall provide at least thirty (30) days advance notice of training opportunities. Online training is always available on the LASA website www.211arizona.org/HMIS.

Data Standards

Policy: Users must enter all data into the HMIS in accordance with the current HUD HMIS Data Standards and the Maricopa County Data Quality Plan.

Procedure: Users must review and understand the most current HUD HMIS Data Standards. The *HUD HMIS Data Standards: HMIS Data Manual* is available on the LASA website www.211arizona.org/HMIS and https://www.hudexchange.info/. Users must review and understand the most current HMIS Data Quality Plan available on the LASA website at www.211arizona.org/HMIS. Failure to comply with these standards will result in the user's license being suspended by LASA until further investigation or training can take place.

Clients

HMIS is a vehicle for information to be passed from participating agency to participating agency regarding client information, services, and referrals. The HMIS is geared to save clients time in re-telling their "story" and providing documentation. At no time should a client's rights, confidentiality or requests be violated.

Denial of Service

Policy: No client shall be denied a service for failure to release information for data sharing purposes or refusal to answer informational questions not required for service eligibility screening.

Procedure: Prior to collecting client-identifying information by the participating agency, clients **must** first sign the Client Acknowledge, acknowledging their request to share or deny the sharing of their information. If the client is returning to the Maricopa HMIS system after an absence of more than one (1) year, client data will be reviewed and updated.

Access to Data

Policy: Clients may have access to their data at any time and can ask for detailed explanation of the information given to them.

Procedure: Clients may request a printed report of their data from the HMIS from a participating agency and requests for data must be made in writing. Agencies will **only** print and distribute information collected by their agency and not all the client's data entered by other agencies and stored in the HMIS. Agencies must comply with client's request within fourteen (14) business days. Clients can ask for and receive a verbal or written explanation of the report given to them by the agency within seven (7) business days of receipt. Clients may request, in writing and including a self-addressed envelope, a printed report from LASA containing all their data in the HMIS. LASA will have thirty (30) days to respond to such requests. Clients can ask for and receive a verbal or written explanation of the report given to them by LASA within seven (7) business days of receipt.

Changing Information

Policy: Clients may request that participating agencies update incomplete and/or incorrect data. However, if an agency believes the request will result in inaccurate data, the agency may deny the request.

Procedure: If the agency chooses not to update the client's information, they must supplement their decision with additional information within the client notes section of the HMIS client record within seven (7) business days of request. Agencies **must** give a written explanation of the decision, which will be copied to the client's file within five (5) business days of decision. When an agency denies a client's request for updating their information, agencies must have a written explanation for refusal in client file within five (5) business days of denial.

Denial of Access

Policy: Participating agencies and LASA reserve the right to deny a client's request to release his/her information if the information is being compiled in reasonable anticipation of litigation or comparable proceedings, contains personal information about another individual not related to the client and/or by disclosure would be reasonably likely to endanger the life or physical safety of any individual.

Educating Clients of Privacy Rights

Policy: The client intake worker, user or case worker will work with the clients to understand their privacy rights, benefits of sharing data and what their data is used for once entered into the HMIS.

Procedure: The Executive Director or his/her designee will ensure that a "Privacy Notice" is posted in an area that is clearly visible to the client. The client must be informed of his/her rights under the privacy policy and should receive a copy of the policy, if requested. The client intake worker, user and case worker will be knowledgeable regarding data sharing policies, release of information policies and how to enter client-level data at the appropriate confidentiality level in the HMIS. LASA is not liable for client-level data that has been entered into the HMIS by a user in which the client's right to privacy was violated.

Communication

From LASA

Policy: LASA is responsible for relevant and timely communication with each participating agency, regarding all aspects of the HMIS, reporting and data standards. All users **must** provide contact information to receive HMIS communication.

Procedure: LASA is not responsible for a participating agency's loss of funds due to their negligence in adhering to any updated HMIS regulations regarding reporting and data collection. General system and training communications from LASA will be directed to all persons enrolled in LASA's HMIS End User distribution list. General communications from LASA will be sent through e-mail communication. Specific communications will be addressed to the person or people involved by direct e-mail communication. For emergency situations, communications will be directed though direct e-mail and the ServicePoint News system located on the home screen of the HMIS.

All FAQs, cheat sheets, documentation, policies, procedures, reporting matrix and general help will be located on the LASA website, www.211arizona.org/HMIS. Agency Administrators are responsible for distributing that information to any additional users at their agency who may need to receive it, including, but not limited to, Executive Directors, client intake workers and data entry specialists.

To LASA

Policy: Questions regarding Code of Ethics agreements, Agency Profile forms and Agency Partnership Agreements should be submitted to LASA. All request forms and update forms are to be submitted to LASA as the System Administrator and HMIS Lead Agency. Users are encouraged to submit HMIS questions through the HMIS help desk, HMISsupport@CIR.org

Procedure: To receive the best customer service from the LASA as the System Administrator, agencies are encouraged to utilize the help desk at HMISsupport@CIR.org or call the help desk at (602) 908-3605. The goal of LASA is to respond to all needs within one (1) business day of first contact.

HMIS Help Desk

Policy: LASA maintains HMIS Help Desk support for assistance on requests including report issues, requests for system enhancements, technical support, helpful hints, training tips, documentation to download, password reset requests, etc.

Procedure: The HMIS Help Desk is available from 9:00 a.m. to 5:00 p.m., Monday through Friday, excluding LASA holidays. Help requests will be addressed in the order of receipt. Help requests will be addressed within twenty-four (24) business hours. All HMIS Help Desk requests received after 4:30 p.m. may be addressed the next business day. To receive the most complete response, requests asking for help to identify or resolve issues with reports **should** have the report in question attached to the request. Submission of HMIS report requests from project representatives will not be accepted though the HMIS Help Desk.

Access

LASA

Policy: LASA will have access to retrieve all data in the HMIS. LASA will not access individual client-level data for purposes other than direct client service-related activities, coordinated assessment, referral, reporting and maintenance, checking for data quality and responding to HMIS Help Desk requests.

Procedure: LASA will be responsible for ensuring that no individual client data is retrieved or distributed for purposes other than direct client service, reporting, system maintenance, performing data quality checks and responding to Help Desk requests. LASA will oversee all reporting to HUD and the public.

All special research requests must be approved by LASA in coordination with requesting agency/initiative. Reports necessary for funding agreements (Annual Performance Reports, Consolidated Annual Performance and Evaluation Reports) may be run at the request of the agency or the request of a federal or state partnering agency.

Agency Administrators

Policy: Agency Administrators will have the ability to access client-level data in all of their agency projects.

Procedure: Participating agency's designated Agency Administrator will have the ability to locate, change, add or remove client-level data from their agency's projects. The Agency Administrator will be able to generate reports for all of their agency's projects. The Agency Administrator will have access to the Annual Homeless Assessment Report. The Agency Administrator will have access to the Provider Information Profile section of the HMIS and will have the ability to change information located within their agency's projects.

User Access

Policy: LASA will assign the most restrictive security settings to all other users not assigned as an Agency Administrator by the Executive Director or their designee.

Procedure: HMIS, in consultation with the agency Executive Director or their designee, will assign appropriate user levels when adding or changing user access. Users will not have the ability to delete or change another project's client-level data. Users will not always have the ability to generate reports for any and all agency projects based on types of user roles. HMIS will always assign the most restrictive access which allows efficient job performance in the interest of client security.

Public Access

Policy: LASA, under the direction of the Maricopa County CoC Board, will address all requests for data from entities other than HMIS Participating Agencies. The public is not given access to the Maricopa HMIS system at any time.

Procedure: The HMIS can enter into data sharing agreements with outside organizations with CoC Board approval for:

- Research
- Data Matching
- Evaluation of Services/Planning.

When Maricopa CoC Board consent is received, LASA and the requested party must consent to a Research Data Sharing Agreement. Research Data Sharing Agreements will require that all parties certify that they will adhere to the strict standards of protecting client-level data employed by the HMIS.

Security

HMIS Software Vendor

System Security

Policy: ServicePoint is supported by the most powerful system security measures available. Using 128-bit encryption, user authentication, and user access levels, ServicePoint ensures that data is protected from intrusion.

Procedure: HMIS Software Vendor' employees, who have access to client-level data, are subject to a national background check, training on confidentiality requirements and must sign a confidentiality statement as part of their employee agreement. The system function logs the time and type of activity, as well as the name of the user who viewed, added, edited or deleted the information.

Servers are located in complexes with:

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

Data Security

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

Procedure: The traffic that flows between the server and the user's workstation is encrypted using the SSL certificate installed on LASA's dedicated servers. Database tape backups are performed nightly. Tape backups are maintained in secure offsite storage. Seven (7) days' backup history is stored on instantly accessible Raid 10 storage. One (1) month's backup history is stored offsite. Users have twenty-four/seven (24/7) access to HMIS Software Vendor emergency line to provide assistance related to outages or downtime.

Unauthorized Access

Policy: If an unauthorized entity were to gain access to the HMIS and client data, or if there were suspicion of probable unauthorized access, LASA and HMIS Software Vendor will take immediate action to protect the security of the system. HMIS Software Vendor will adhere to the "Securing Client Data" manual (Attachment D).

Procedure: The system would be examined to determine the presence of system or data corruption. If the system has been compromised, the system would be taken offline. Using the previous night's backup, a restored copy of the system data would be loaded onto another server and the system brought back online with the back-up copy. Comparing the back-up database to the database taken offline, an investigation would be launched to determine the extent of the unauthorized activity/corruption and the corrective action needed. Upon completion of the investigation, findings would be reported to LASA and options would be discussed. Upon LASA's approval, corrective action would be initiated. Corrective action could include all or part of the following:

- The original hard drive would be completely erased and rebuilt, including a new operating system, SSL Certificate, applications and the back-up database.
- If applicable and feasible, lost data from the original database would be restored.

If HMIS Software Vendor or its employees are determined to be at fault for unauthorized access, LASA may terminate the ServicePoint License and Service Agreement and pursue legal remedies.

Licensed Users

A licensed user is a person who has signed and submitted a HMIS Code of Ethics Agreement and it is still in effect for the current year. If LASA is not notified of their termination from the agency within twenty-four (24) hours of termination, neither HMIS Software Vendor or LASA as the System Administrator and HMIS Lead Agency will be liable for actions of a former agency employee with an active license. The Agency shall be liable and LASA may terminate access to the HMIS if it determines that the Agency acted carelessly in managing their licensed users.

User Access

Policy: LASA will provide unique usernames and initial passwords to each licensed user. Usernames and passwords may not be exchanged or shared with other users.

Procedure: LASA will provide directly to the user a unique username and initial password upon completion of training requirements as stated in this manual. LASA will have access to the list of usernames. LASA will perform an annual user audit for invoicing and licensing proposes. The sharing of usernames will be considered a breach of the HMIS User Agreement and the Partnership Agreement. Exchanging usernames seriously compromises security and accountability to clients. If a breach occurs, it may subject the agency to discipline and termination of access to the HMIS. LASA will randomly audit 2% of users a month to monitor that users are following the Maricopa HMIS Code of Ethics.

Passwords

Policy: Users will have access to the HMIS via a username and password. Passwords will be reset every forty-five (45) days. Passwords must consist of at least eight (8) characters and include at least two (2) digits. Users must keep passwords confidential.

Procedure: On the forty-fifth (45th) day when the user logs in, the system will require the user to create a new password and enter it twice before accessing the database.

The sharing of passwords will be considered a breach of the HMIS User Agreement. If a breach occurs, LASA may subject the agency to discipline and termination of access to the HMIS.

Password Recovery

Policy: Agency Administrators may reset passwords. If the Agency Administrator is unavailable or otherwise unable to reset a password for an end user, LASA will reset a user's password in the event the password is forgotten.

Procedure: Users must request a password reset by submitting a request to the HMIS Help Desk at HMISsupport@cir.org or by calling the HMIS Help Desk at (602) 908-3605.

LASA will verify the user is active in the system prior to resetting a password. The reset information will be sent back to the user via the Help Desk. The user must enter the password given. The system will only accept this password one time. The system will require the user to create a new password and enter it twice before accessing the database.

Location of Data Access

Remote Access

Policy: Users will ensure the confidentiality of client data, following all security policies in the HMIS Policies and Procedures Manual and adhering to the standards of ethical data use, regardless of the location of the connecting computer. The Executive Director or designee has the responsibility to assure the user is in compliance with this and all other policies, procedures, agreements and rules governing the HMIS.

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

Examples of allowable Remote Access:

- Personal laptops that were not purchased by the agency.
- Access to the HMIS on a private network other than that of the agency.
- Private home desktops.

Procedure: LASA may audit remote access by HMIS users. If a user is found to have accessed the HMIS through an unsecured network, the user license will be immediately suspended. LASA may impose additional sanctions on the agency including termination of access to the HMIS.

Agency Data

Data Retrieval

Policy: HMIS -participating agencies will have access to retrieve any individual client-level data and aggregate data for their own projects. Participating agencies will not have access to retrieve client-level or aggregate data for other participating agencies or system-wide.

Procedure: Agency Administrators using the ServicePoint available Reports or ART will only be able to extract data from those records to which they have access based on their level of security given by LASA. Whenever a user attempts to access an aggregate report for an unauthorized agency, the report will show "0" or be inaccurate due to the security level of the user. Both ServicePoint available Reports and ART will limit the user access and only report data from records to which the individual user has access.

Extracted Data

Policy: HMIS -participating agencies have access to retrieve any individual client-level data and aggregate data for their own projects and download the information onto a local storage vessel. Users will maintain the security of any client data extracted from the database and stored locally, including data used in custom reporting.

Procedure: Any data printed or downloaded from HMIS is protected data and should be held in secured paper or electronic files. All extracted data falls within the same confidentiality procedures as electronically-stored data. LASA is not responsible for breaches in data once removed from the HMIS. If a participating agency's licensed user or Agency Administrator extracts data, the participating agency for which the licensed user works is responsible for any data breach on data extracted by the user and may result in termination of HMIS access by LASA.

Compliance Security Review

Policy: HMIS -participating agencies are subject to random or scheduled compliance monitoring review by LASA as outlined in the HMIS Data Quality Plan.

Procedure: All agencies will be desk-monitored at least once a year for security risks and compliance with documentation. On-site monitoring will be conducted at least once yearly for agencies under contract with the Maricopa County CoC. Agencies not under contract with the Maricopa CoC will be monitored if they are deemed to be a high or medium security risk based on the annual desk monitoring.

HMIS Data Sharing

Agencies are able to share client information with agencies outside of their network with appropriate client authorization. The HMIS is a vehicle through which agencies can share data outside of their own agency and network. County-wide reporting is based on aggregate, non-identifying data; therefore, aggregate, non-identifying data may be shared with the public without specific permission. These polices would be made clear to clients as part of the Client Acknowledgement and Release of Information form. Data sharing protocols will be further described in the HMIS Privacy Plan (Attachment F).

Opt-In

Policy: All agencies and projects, with exception of HOPWA, domestic violence service providers and those that fall within Federal Regulation 42 CFR Part 2 (those that receive federal funds for substance abuse treatment services as a licensed treatment facility), may share client-level data with other HMIS -participating agencies by executing a written and approved Data Sharing Agreement or MOU. A copy of the Data Sharing Agreement or MOU must be signed by all parties and kept on file at LASA. Verbal agreements will not be accepted. The HMIS currently shares the HUD Universal Data Elements (UDEs) continuum-wide.

Procedure: The participating agency's Executive Director or designee is responsible for ensuring that all licensed users within the agency abide by all the policies and procedures stated within all signed documents including the Data Sharing Agreement or MOU. Each participating agency will retain a copy of the agreement and a master will be filed with LASA. All clients must have a valid Client Acknowledgement Form in their case file prior to users entering client-level data into the HMIS to indicate either approval or denial of sharing their data.

Opt-Out

Policy: Agencies can request to be removed from data sharing. LASA and the Maricopa County CoC Board reserve the right to deny a request to opt-out of data sharing.

Procedure: Any agency Executive Director or designee wishing to opt-out of data-sharing must execute a HMIS Data Sharing Exit Agreement. LASA will make a final decision within seven (7) business days of receipt of agreement. Data share historically cannot be reversed due to software regulations.

If approved:

1. Agency will retain a copy of the agreement and a master will be filed with LASA.
2. LASA will remove the data sharing privileges within three (3) days of approval.
3. Once data sharing is removed, agency users will no longer be able to grant permission based on appropriate client consent to share individual client information.
4. Authorized, licensed users will only be able to view their own agency's client data.
5. The client's ID, name, year of birth, veteran status and Social Security Number, alias, will remain at a global sharing level to limit duplicate clients in the system.

If denied:

1. Agency will retain a copy of the agreement and a master will be filed with LASA.
2. Agencies can appeal the decision to the CoC Board in a written statement within three (3) business days from receipt of decision.

Visibility Settings

Policy: All data sharing policies will be enforced by LASA.

Procedure: Each user's access to data will be defined by their user type, as described in the Access section of this manual. LASA will conduct at least annual file checks for appropriate client authorization and will conduct random monthly audit reports for 2% of all HMIS users.

Client Denial to Share

Policy: If the client chooses not to have their data shared with other agencies and the agency participates in data sharing, the data **must** be locked in the system to restrict visibility to the agency which originally entered the information.

Procedure: The user **must** contact the HMIS Help Desk prior to entering client-level data into the HMIS. LASA as the System Administrator is responsible for locking client-level data with the correct visibility security settings. LASA will monitor for client denial to share in desk-monitoring and on-site monitoring.

Scanned Document Management

Policy: LASA is responsible for organization and management of the HMIS. It is necessary to follow standardized procedures to upload documents to ensure uploaded information is useable system-wide.

Procedure: Documents uploaded to a client must have the naming standards of:

- Client ID#, Document Title, Date Saved
  - ✓ Example: *123456, Homeless Verification, 11/20/2013*

File attachments may only be uploaded to the client profile screen under "File Attachments". Users may never remove documents of another agency and may only remove theirs when uploading an updated version. Unless otherwise noted by client denial, all file attachments will be shared by agencies sharing data.

Data Shared Information

Policy: The sharing standard for each area of HMIS data entry is set forth in the HMIS Release of Information (Attachment C) and Privacy Plan (Attachment F). The intent of the HMIS is to allow as much data sharing as appropriate and necessitated by clients' needs and services provided to meet those needs.

Procedure: The HUD Universal Data Elements (UDEs) are shared Continuum-wide. All other data sharing will be noted in the HMIS Data Share plan.

Data at no time is currently to be shared outside the agency regarding:

- HOPWA Projects
- RHY Projects
- Youth Under 18

Data Quality

The data standards established by HUD and LASA are applied to all projects reporting client-level data in the HMIS. At no time do standards increase or decrease with the source of funding for the project. To have correct, accurate and reliable reporting in a timely manner, all projects **must** adhere to the policies and procedures established. Please refer to the HMIS Data Quality Plan available on the LASA website at www.211arizona.org/HMIS

License Suspension and/or Replacement

Policy: At any time, LASA reserves the right to suspend a user's or agency administrator's license if having difficulty entering client-level data and providing accurate reports after appropriate trainings. LASA can recommend and require the Executive Director or designee to assign a different staff member or volunteer to attend training and become a participating agency user to enter client-level data.

Violation of Data Quality and Integrity

Policy: In its discretion, LASA may report violations with the Maricopa HMIS Data Quality plan and breaches in data integrity to the CoC Lead and may result in termination of HMIS access by LASA.

Procedure: Such action will be conducted in accordance with the HMIS Policies and Procedures Manual.

Licensing and Invoicing

LASA as the HMIS Lead Agency invoices all provider agencies annually in the first quarter of the fiscal year for HMIS user fees. Invoicing occurs after the annual user audit for each participating agency is completed. The annual user license fee is recommended by LASA based on the HMIS Software Vendor software contract and approved by the Maricopa County CoC Board. The funds received for the annual user license assists with paying for the user license fees as part of the HMIS Software Vendor contract and provides match for the HMIS Lead HUD grant.

Annual Invoice

Policy: LASA will send an invoice to each Executive Director or designee of each agency or the appropriate staff at a partnering federal or state agency.

Procedure: Invoices will be mailed. Payments are due within thirty (30) days of receipt of invoice. Non-payment of licenses may result in suspension by LASA. LASA will make all project representatives aware of agencies that have had their user licenses suspended. The User Fee is a flat fee as determined by the software contract and therefore will not be pro-rated when new user licenses are purchased throughout the year

Grievances

From a Participating Agency or Client to the HMIS

Policy: HMIS participating agencies have the right to file a grievance against LASA as the System Administrator and HMIS Lead Agency. Clients have the right to file a grievance against a participating agency regarding the HMIS.

Procedure: LASA will respond within thirty (30) days to complaints from families, owners, employees and members of the public. All complaints must be submitted in writing and will be documented.

- Categories of Complaints
  - ✓ Complaints from clients: a client disagrees with an action or inaction of the Maricopa HMIS Lead.
  - ✓ Complaints from participating agencies or other HUD-funded programs: a HMIS -participating agency, a HUD-funded program or other federal-funded program disagrees with an action or inaction of the HMIS Lead.

The complaining party will submit the complaint in writing to LASA within seven (7) business days of the date of occurrence. It is LASA's objective to resolve disputes at the lowest level possible and to make every effort to avoid the most severe remedies. However, if this is not possible, LASA will ensure that applicants and participants will receive all of the protections and rights afforded by the law and applicable regulations.

Participation Termination

Initiated by the Participating Agency

Policy: In the event of termination of the HMIS Partnership Agreement, all data entered into the HMIS will remain an active part of the HMIS and the records will retain their original security settings.

Procedure: HUD-funded agencies are required to participate in the HMIS. For those participating agencies that are non-HUD-funded, the person signing the initiating HMIS Partnership Agreement will notify LASA with a date of termination in writing. In all cases of termination of the HMIS Partnership Agreement, LASA will deactivate all users from the agency on the date of termination stated by the agency. All client-level data entered into the HMIS will remain an active part of the HMIS and the records will retain their original security settings.

Initiated by LASA

Policy: LASA will terminate the HMIS Partnership Agreement for non-compliance with the terms of that agreement.

Procedure: HUD-funded agencies are required to participate in the HMIS. For those that are terminated, this will be reported to the Maricopa County CoC Lead. For those participating agencies that are non-HUD-funded, LASA will notify the person signing the initiating HMIS Partnership Agreement with a date of termination in writing. LASA will give thirty (30) days written notice to the agency, regardless of funding source, to the attention of the person who initiated the agreement. LASA requires any HMIS violations to be rectified before the HMIS Partnership Agreement termination is final. LASA may also terminate the HMIS Partnership Agreement without cause upon thirty (30) days written notice to the participating agency.

In all cases of termination of the HMIS Partnership Agreement, System Administrator will make inactive all users from the agency on the date of termination. All client-level data entered into the HMIS will remain an active part of the HMIS, and the records will retain their original security settings.

Projects in HMIS

Adding a New Project in HMIS by Participating Agency

Policy: The Executive Director or designee will notify LASA thirty (30) days prior to implementation of a new project.

Procedure: At least thirty (30) days prior to anticipated implementation date, the Executive Director or designee will meet with LASA to fill out the New Project Form (Attachment J)

Making Changes to Existing Projects in HMIS

Policy: The Executive Director or designee will notify LASA of programmatic changes.

Procedure: The Executive Director or designee will notify LASA of any applicable programmatic changes to existing programs which may have an effect on data collection, data entry, data quality or data reporting at least forty-five (45) business days prior to the implementation date of the change. Recommendations and timelines for the changes will be returned to the participating agency no more than ten (10) business days from receipt date of request. LASA will complete changes at least seven (7) business days prior to the implementation date for final approval from the participating agency.

Additional Customization

Policy: The participating agency will be solely responsible for additional database customization costs. This includes the voluntary transfer of existing grant client-level data and custom build reports beyond that of LASA scope of work.

Procedure: The Agency Administrator or Executive Director or designee will notify LASA of any applicable programmatic customization which may have an effect on data collection, data entry, data quality or data reporting at least forty (40) business days prior to the implementation date of the change. Proposed customization and/or changes must be submitted in writing.

If support from HMIS Software Vendor is necessary to make the changes, LASA will communicate to the HMIS Software Vendor the needs and scope of work for the participating agency. Recommendations and timelines for the changes will be returned to the participating agency no more than ten (10) business days from receipt date of request, including a Statement of Work from the Software Vendor, if applicable. LASA will complete changes at least seven (7) business days prior to the implementation date for final approval from the participating agency. If a participating agency voluntarily transfers an existing grant to another agency, LASA will not pay for client-level data to be transferred. The agency requesting the transfer will be liable for any fees incurred.

Acknowledgement of Receipt of the HMIS Policies and Procedures Manual

By signing this form, you acknowledge receipt of the HMIS Policies and Procedures Manual from Community Information and Referral Services (LASA). Your signature further certifies that you have read, understand and will abide by the policies and procedures, as detailed in this document, as well as accept any measures taken for violation of these practices. Please note, the HMIS Policies and Procedures Manual is subject to change.

_____
Signature of Licensed User

_____ _____
Print Name Date

_____
Signature of Executive Director

_____ _____
Printed Name of Executive Director Date

Return signed form to LASA:

Via e-mail:
HMISsupport@cir.org

Via mail:
Community Information and Referral Services
Attn: HMIS
2200 North Central Ave, #211
Phoenix, AZ 85004

ATTACHMENT A – Maricopa HMIS Partnerships Agreement

HMIS Partnership Agreement

This agreement is entered into on the _____th day of _____, 20__ between Community Information and Referral Services, hereafter known as "CIR", and _____ (Agency Name) hereafter known as "Provider Agency" regarding access and use of the Maricopa Homeless Management Information System, hereafter known as the "Maricopa HMIS".

I. Introduction

Maricopa HMIS, a shared homeless database, allows authorized Provider Agencies throughout the geographic area of Maricopa County to input, use, and receive information concerning their own clients and to share information, subject to agreements, on common clients.

Maricopa HMIS Goals include:

a) People who are homeless or are in need of homeless prevention assistance will receive improved coordinated care / services.

b) Participating providers will improve their data collection and workflow with use of HMIS

c) Participating providers will use the HMIS to meet all current external homeless/homeless prevention reporting requirements from HUD and non-HUD funding sources.

d) The community will have timely, credible, quality data about services and people who are homeless or in threat of becoming homeless.

e) 100% of homeless providers will participate in the HMIS. (Excluding Domestic Violence Providers)

f) HMIS will be user-friendly for providers

g) Community and provider agency stakeholders will have current accurate information about HMIS implementation and data regarding homelessness in Maricopa County

CIR administers Maricopa HMIS, contracts for an agency to house the HMIS database central server and coordinates Provider Agency access to the HMIS database. CIR shall protect Maricopa HMIS data from accidental or intentional unauthorized modification, disclosure, or destruction. Maricopa HMIS, when

used correctly and faithfully, will improve knowledge about homeless people--their services and service needs, and may result in a more effective and efficient service delivery system.

II. Confidentiality

A. The Provider Agency will uphold relevant federal and state confidentiality regulations and laws that protect client records and will only release confidential client records with written consent by the client[1], or the client's guardian[2], unless otherwise provided for in regulations or laws.

1. The Provider Agency will abide specifically by federal confidentiality regulations as contained in the Code of Federal Regulations, 42 CFR Part 2, regarding disclosure of alcohol and/or drug abuse records if applicable. In general terms, the federal regulation prohibits the disclosure of alcohol and/or drug abuse records unless disclosure is expressly permitted by written consent of the person to whom it pertains or as otherwise permitted by 42 CFR Part 2. A general authorization for the release of medical or other information is not sufficient for this purpose. The Provider Agency understands the federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patients.

2. The Provider Agency will abide specifically, when applicable, with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and corresponding regulations passed by the Federal Department of Health and Human Services. In general, the regulations provide consumers with new rights to control the release of medical information, including the right: to give advance consent prior to disclosures of health information; to see a copy of health records; to request a correction to health records; to obtain documentation of disclosures of health information; to obtain an explanation of privacy rights and to be informed about how information may be used or disclosed. The current regulation provides protection for paper, oral and electronic information.

3. The Provider Agency will abide by Arizona State Laws and Federal Laws related to confidentiality and security of medical, mental health and substance abuse information as found in Arizona Revised Statues Title 12, Arizona Revised Statutes Title 36, 42 CFR Part 2 and other relevant statutes, rules and regulations as applicable.

4. The Provider Agency will provide a verbal explanation of Maricopa HMIS and arrange, when possible, for a qualified interpreter or translator for an individual not literate in English or having difficulty understanding the consent form(s).

[1] Anyone who receives services from a Provider Agency.
[2] "Guardian" is anyone legally in charge of the affairs of a minor or of a person deemed incompetent, according to and defined in Title 14 of the laws of the State of Arizona. All references to "client" in this Agreement also apply to "client's guardian."

5. The Provider Agency will not solicit or input information from clients into Maricopa HMIS unless specific information proves essential to provide services, to develop reports and provide data, and/or to conduct evaluations and research. Evaluation and research will only use de-identified client data except in the case when the Provider Agency evaluates and researches its own clients. In all cases, the Provider Agency shall maintain compliance with all state and federal laws regarding research, evaluation and confidentiality of individual client identities.

6. The Provider Agency will not divulge any confidential information received from the Maricopa HMIS to any organization or individual without proper written consent by the client (or guardian where appropriate) unless otherwise permitted by relevant regulations or laws.

7. The Provider Agency will ensure that every person issued a User Identification and Password to the Maricopa HMIS will comply with the following:

    a. Read and abide by this Partnership Agreement
    b. Read and sign the HMIS Code of Ethics form[3]
    c. Create a unique User I.D. and password; and will not share or reveal that information to anyone by written or verbal means

8. The Provider Agency understands that individuals granted Agency Administrator access within each agency must become a Designated Maricopa HMIS Agency Administrator through specific training provided by the CIR. The Provider Agency understands that all client information will be encrypted on a file server physically located in a locked office with controlled access, at the offices of HMIS Software Vendor, LLC located at 333 Texas Street, Suite 300, Shreveport, Louisiana 71101.

9. The Provider Agency agrees to submit payments in a timely fashion to CIR for annual HMIS User License fees in effect at the time of execution of the agreement.

   CIR agrees to work with Provider Agency Administrators to reconcile any discrepancies on annually generated User License Invoices.

B. The Provider Agency agrees to document a client's (or guardian's when appropriate) understanding and consent to enter client information into a central database and the reasons for this entry. Furthermore,

1. An individual client (or guardian) must give implied or informed client consent by understanding and signing a consent form for the Provider Agency prior to the Provider Agency sharing any client information to another agency.

2. The completed consent form provides:

[3] See Code of Ethics form

a. Informed client consent regarding basic identifying client data to be entered into a shared database
b. Release of non-confidential service transaction information to be shared for report purposes.
c. Client release to authorize the sharing of basic client identifying information among designated Maricopa HMIS Provider Agencies.

3. A client might deny authorization to share basic identifying information or other specified information via Maricopa HMIS. The Client Profile section within ServicePoint will be marked restricted. This allows only the entering Provider Agency access to client information and precludes the ability to share information.

4. Each Provider Agency is responsible for ensuring that its staff and users comply with the requirements for informed consent and client confidentiality.

5. The Provider Agency agrees to place all client consent forms related to Maricopa HMIS in a file to be located at the Provider Agency's business address and that such forms are made available to the CIR for periodic audits. The Provider Agency will retain these Maricopa HMIS related consent forms for a period of five years upon expiration, after which time the forms will be discarded in a manner ensuring un-compromised client confidentiality.

6. The Provider Agency understands that in order to update, edit, or print a client's record, the Provider Agency or SubProvider Agency must have on file current client consent form.

   The Provider Agency agrees to enter the minimum data required in the Maricopa HMIS; however, this does NOT mean that a Provider Agency is required to share client identifiable information. A client's information may be restricted to overall access when the client refuses to allow his/her name, social security number or other personally identifiable information to be shared in the database.

7. The Provider Agency agrees to permit the Maricopa HMIS Project to initiate and administer the following data share with all HMIS participating agencies. A listing of participating agencies can be found on the Maricopa HMIS website at www.211arizona.org/hmis.

   Data will be shared for the purpose of coordinated assessment and service coordination. The data shared will help decrease duplication of work between participating organizations, increase the quality of the data being entered in HMIS, decrease the intake processes for homeless clients, and provide a more client centric data system. The data share will help the Continuum make clearer data based decisions while performing a more efficient delivery of service.

The Provider Agency agrees to share Continuum determined data share elements and Continuum determined coordinated assessment tools. A listing of the items can be viewed on the Maricopa HMIS website at www.211arizona.org/hmis.

8. The Provider Agency can also sign a Memorandum of Understanding (MOU) with other HMIS Providers in order to share additional data. The ability to share client level data will help each Provider Agency from duplicating received services.

   The addition of new data elements into the data share after the MOU is signed will require written approval from each Provider Agency. An email will be sent by the Maricopa HMIS Project to each Provider Agency to detail the changes to the data share and request a return email to acknowledge the changes. This email response will be sufficient documentation of approval.

III. Data Entry and/or Regular Use

A. User Identification and Passwords are not permitted to be shared among users.

B. If a Provider Agency has access to a client's basic identifying information, non-confidential service transactions and confidential information and service records, it will be generally understood that a client gave consent for such access. However, before a Provider Agency can update, edit, or print such information, it must have informed client consent in writing

C. Provider Agency will not enter any fictitious or misleading client data on an individual or family in Maricopa HMIS.

D. The Provider Agency will not misrepresent the number of clients served or the type of services / beds provided in Maricopa HMIS by entering known, inaccurate information (i.e. Provider Agency will not purposefully enter inaccurate information on a new record or to over-ride information entered by another agency).

E. The Provider Agency will enter information into Maricopa HMIS according to agency and HMIS adopted standards and will strive for real-time, or close to real-time, data entry. Real-time or close to real-time is defined by either immediate data entry upon seeing a client, or data entry into Maricopa HMIS within one business day. This assumes that the Provider Agency has sufficient computers available for all staff performing data entry into Maricopa HMIS.

F. The Provider Agency understands that with a current standard Maricopa HMIS client consent form on file, it can update, edit, and print a client's basic identifying information.

G. Discriminatory comments by an employee, volunteer, or other person acting on behalf of the Provider Agency based on race, color, religion, national origin, ancestry, handicap, age, sex, and sexual orientation are not permitted in Maricopa HMIS. Offensive language and profanity are

not permitted in Maricopa HMIS. This does not apply to the input of direct quotes by a client IF the Provider Agency believes that it is essential to enter these comments for assessment, service and treatment purposes.

H. The Provider Agency will utilize the Maricopa HMIS for business purposes only.

I. The Provider Agency understands CIR will provide initial training and periodic updates to that training to assigned Provider Agency staff about the use of Maricopa HMIS. This information is to then be communicated to other staff using Maricopa HMIS within the Provider Agency.

J. The Provider Agency understands CIR will provide a help desk with Technical-support according to the following:

Help Desk will be provided between 9:00 a.m. to 5:00 p.m. Arizona Time. Support telephone numbers and email addresses will be provided to Provider Agencies upon signing this Agreement. CIR will ensure that any support calls are responded to according to the Severity Code Response Time, provided that all available numbers and e-mail addresses have been accessed. Contact with the Help Desk will not incur any long distance charges.

In the event of non-response the Provider Agency should notify the System Administrator at CIR.

K. The Provider Agency will keep updated virus protection software on agency computers that access Maricopa HMIS[4].

L. Transmission of material in violation of any United States federal or state law or regulation is prohibited and includes, but is not limited to: copyright material, material legally judged to be threatening or obscene, and material considered protected by trade secret.

M. The Provider Agency will not use Maricopa HMIS with intent to defraud the federal, state or local government or an individual entity, or to conduct any illegal activity.

N. The Provider Agency acknowledges that other agencies will periodically have access to de-identified data on the central database. To ensure the information generated by or through Maricopa HMIS presents an accurate picture of homelessness and services to homeless people in Maricopa region, the Provider Agency will enter data in a timely and accurate manner.

O. Each Provider Agency assumes responsibility for (its) staff and users' compliance in regards to requirements for data entry and use of Maricopa HMIS. To assess the quality of data and reports

[4] Provider Agency assumes financial responsibility for virus protection software.

generated by the system, CIR[5] will conduct periodic monitoring and reviews on data. These include and are not limited to the following:

1. Quality of data entered by Provider Agency

    a. Inappropriate and/or duplicate records
    b. Untimely and/or inaccurate information
    c. Missing required data elements

2. Operation of the software

3. Reporting functionality

P. Provider Agency's must notify CIR in writing of any changes to User ID including, but not limited to, new personnel, and released or terminated personnel.

IV. Reports

A. The Provider Agency understands that it will retain access to all identifying and statistical data on the clients it serves.

B. The Provider Agency understands that it may have access to personally identifiable client information even if the Provider Agency has not served the client. The Provider Agency agrees to **not report or release** any identifiable client information on clients that the Provider Agency has not served.

C. The Provider Agency will run its own reports from Maricopa HMIS. Each Provider Agency will receive required training and then have the ability to complete each Provider Agency's reporting needs.

V. Proprietary Rights and Database Integrity

A. The Provider Agency and CIR understand Maricopa HMIS and CIR are custodians of data, and not owners of data. The database is jointly owned by the Provider Agency and the Continuum of Care Regional Committee on Homelessness.

1. In the event Maricopa HMIS ceases to exist, CIR will notify Provider Agencies and provide a six-month time period for the Provider Agencies to access and save specific client data, statistical data and frequency data from the entire system. Then, the centralized server database will be purged or stored. If the latter occurs, the data will remain in an encrypted and aggregate state.

[5] CIR may conduct these reviews or may accept a similar review by another organization as evidence of compliance by the Provider Agency.

2. In the event CIR ceases to operate Maricopa HMIS, another organization will administer and take custodianship of the data. The CIR or its successor Agency will inform, in a timely manner, all Provider Agencies.

3. If the Provider Agency ceases to exist, it shall notify and work with CIR to determine the appropriate disposition of Provider Agency's data, including the transfer of the data to a successor agency.

4. If the Provider Agency chooses to withdraw from Maricopa HMIS, the Provider Agency shall notify CIR of intended withdrawal date. CIR shall allow sixty days for the Provider Agency to access and save agency specific client data, statistical data and frequency data from the entire system. The Provider Agency is financially responsible for extracting its data.

B. The Provider Agency will not give or share assigned user identification and passwords to access Maricopa HMIS with any other organization, governmental entity, business, or individual.

C. The Provider Agency will not cause in any manner, or way, corruption of Maricopa HMIS. Any unauthorized access or unauthorized modification to computer system information or interference with normal system operations, whether on the equipment housed by CIR or any computer system or network related to Maricopa HMIS will result in immediate suspension of services and CIR will pursue all appropriate legal action.

D. The CIR[6] will ensure and conduct periodic monitoring and reviews with Provider Agencies to enforce informed and implied consent standards, HUD Standards, and Continuum of Care Regional Committee on Homelessness Standards including:

1. Appropriate documentation indicating client awareness and consent of data being entered into central database

2. Consent to release certain information.

3. Appropriate entry of universal and programmatic data elements as defined by HUD

4. Adherence to HMIS Policies and Procedures including Security Standards.

VI. Hold Harmless

A. CIR makes no warranties, expressed or implied. The Provider Agency, at all times, will indemnify and hold CIR harmless from any damages, liabilities, claims, and expenses that may be claimed against CIR or the Provider Agency, or for injuries or damages to CIR or the Provider Agency arising from Provider Agency's participation in Maricopa HMIS, or arising from any acts, omissions, neglect or fault of the Provider Agency or its agents, employees, licensees, or

[6] The CIR may conduct these reviews or may accept a similar review by another organization, designated by CIR, as evidence of Provider Agency compliance.

clients, or arising from the Provider Agency's failure to comply with laws, statutes, ordinances or regulations applicable to it or the conduct of its business. CIR shall not be liable to the Provider Agencies for damages, losses, or injuries to the Provider Agencies or another party unless such is the result of negligence or willful misconduct of CIR or its agents, employees, licensees or clients.

B. The Provider Agency makes no warranties, expressed or implied. CIR, at all times, will indemnify and hold the Provider Agency harmless from any damages, liabilities, claims, and expenses that may be claimed against CIR or Provider Agency, or for injuries or damages to CIR, the Provider Agency, or another party arising from participation in Maricopa HMIS, or arising from any acts, omissions, neglect, or fault of CIR or its agents, employees, licensees, or clients, or arising from CIR's failure to comply with laws, statutes, ordinances or regulations applicable to it or the conduct of its business. Thus CIR will also hold the Provider Agency harmless for negative repercussions resulting in the loss of data due to delays, non-deliveries, mis-deliveries, or service interruption caused by CIR or a Provider Agency's negligence or errors or omissions, as well as natural disasters, technological difficulties, and/or acts of God. The Provider Agency shall not be liable to CIR for damages, losses, or injuries to CIR or another party unless such is the result of negligence or willful misconduct of the Provider Agency or its agents, employees, licensees or clients.

C. The Provider Agency agrees to keep in force a comprehensive general liability insurance policy with combined single limit coverage of not less than one million dollars ($1,000,000). Said insurance policy shall include coverage for theft or damage of the Provider Agency's Maricopa HMIS-related hardware and software.

VII. CIR Responsibilities

A. CIR agrees to enter into a contract and maintain the services of the ServicePoint software according to the terms and conditions of the contract with the Software Provider.

B. CIR agrees to maintain a Project Manager who will provide training, implementation, help desk and support to the Provider Agency and SubProvider Agencies.

VIII. Dispute Resolution and Appeals

A. If the Provider Agency disagrees with any element of this Agreement it shall make every effort to address and resolve those issues with the Chief Executive Officer of the CIR.

B. If CIR and the Provider Agency are unable to reach a solution, either party may raise the issue to the HMIS Advisory Board for a solution.

C. The HMIS Advisory Board will make every effort to resolve the issue; however, if the issue cannot be adequately resolved at this level, the HMIS Advisory Board shall recommend a process to reach resolution.

IX. Terms and Conditions

A. The parties hereto agree that this Agreement is the complete and exclusive statement of the agreement between parties and supersedes all prior proposals and understandings, oral and written, relating to the subject matter of this Agreement.

B. Neither party shall transfer or assign any rights or obligations without the written consent of the other party.

C. The exception to this term is if allegations, or actual incidences, arise regarding possible, or actual, breeches of this agreement. Should such situation arise, the CIR may immediately suspend access to the Maricopa HMIS until the allegations are resolved in order to protect the integrity of the system.

1. When the CIR becomes aware of a possible or actual incident, it shall make a reasonable effort to address its concerns with the Executive Director of the Provider Agency prior to taking action.

2. If CIR believes that the breech by a Provider Agency is such that it may damage the integrity of the central database and the information in the central database for the Provider Agency or any other Agency, it may take immediate steps to suspend the Provider Agency's access to HMIS prior to addressing the concerns with the Director of the Provider Agency. CIR will then address the concern with the Director of the Provider Agency to resolve the issue.

3. Action with a Provider Agency may include the provision of training and technical assistance, fines, suspension of access to the central database or other appropriate measures to ensure that the data integrity is maintained.

D. If a Provider Agency believes that action taken is not appropriate, or it cannot meet the conditions of the decision, it may appeal the action to the HMIS Advisory Board. If the Advisory Board and the Provider Agency cannot reach agreement, a representative of the Advisory Board, CIR and Provider Agency shall address the issue before the Continuum of Care Regional Committee on Homelessness. Decisions by the Continuum of Care Regional Committee on Homelessness are final; however, every attempt will be made by all parties to reach a reasonable accommodation for the Provider Agency.

E. This agreement may be modified or amended by written agreement executed by both parties with 30 days' advance written notice.

F. Use of Maricopa HMIS constitutes acceptance of these Terms and Conditions.

IN WITNESS WHEREOF, the parties have executed this Agreement on the year and day first above written.

COMMUNITY INFORMATION AND

REFERRAL SERVICES

_____

(Signature)

_____

Title

_____

Date

PROVIDER AGENCY

_____

(Signature)

_____

Title

_____

Date

ATTACHMENT B – 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

ATTACHMENT C – Release of Information

Maricopa Regional Continuum of Care Client Data Sharing Release of Information

The Maricopa Regional Continuum of Care authorizes providers to utilize data systems, which currently include the Homeless Management Information System (HMIS) and coordinated entry data systems such as Homelink, working together to provide services for those experiencing homelessness. The benefit of sharing your client information is that it will allow us to assist in planning for and providing services to you, the client. This information will be shared among agencies to provide coordination and delivery of your services. Know that all information entered into these databases is protected by passwords, encrypted technology, or other means. Steps are taken to safeguard the information that is entered into the system but no system is infallible.

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

The following data elements will be shared:

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

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

- **Other agencies may join this collaboration in the future and an updated list can be found at www.211arizona.org/HMIS.**

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

- I have received a copy of The Privacy Notice, which describes the ways in which the primary identifying information, and other client data information may be used or disclosed.
- I have the right to ask questions about this form and anything that I do not understand around data sharing.
- **I have the right to opt-out of having information shared with other participating agencies and still receive services from that agency. I am still eligible services if I do not consent to data sharing.**
- I have the right to revoke this consent at any time by completing the Client Revocation Form. I understand that the data provided by me will still be available to any agency where I have received services in the past.

As applicable, I agree to share my information and the information of my family members.

Minor Children (if any):
Child's name: _____ DOB _____ Last 4 digits of SS _____
Child's name: _____ DOB _____ Last 4 digits of SS _____
Child's name: _____ DOB _____ Last 4 digits of SS _____
Child's name: _____ DOB _____ Last 4 digits of SS _____

☐ **Please indicate by initialing here if you DO NOT AGREE to share your information.**

_____ _____
Client Signature Date Other party (guardian) Date

_____ _____
Print Name Relationship to client

_____
Staff Signature Date

_____ _____
Print Name of Organization Print Name of Organization Staff

ATTACHMENT D

BOWMAN SYSTEMS SECURING CLIENT DATA

© 2014 Bowman Systems L.L.C. All Rights Reserved.

This document and the information contained herein are the property of Bowman Systems L.L.C. and should be considered business sensitive.

Bowman Systems® and the Bowman Systems® logo are trademarks of Bowman Systems L.L.C. All other brand or product names are trademarks or registered trademarks of their respective holders.

All agency and client names depicted herein are completely fictitious. No association with any real organization or persons is intended or should be inferred.

Bowman Systems
333 Texas Street, Suite 300
Shreveport, LA 71101
Toll Free: (888) 580-3831
Direct: (318) 213-8780
Fax: (318) 213-8784
www.bowmansystems.com

BOWMAN systems

TABLE OF CONTENTS

ACCESS SECURITY 2
BOWMAN SYSTEMS EMPLOYEES 2
BOWMAN SYSTEMS ACCESS TO SERVICEPOINT 2
AUDIT TRAIL 3
CUSTOMER ACCESS TO SERVICEPOINT 3
SITE SECURITY 4
BUILDING SECURITY 4
BOWMAN SYSTEMS HEADQUARTERS SECURITY 4
NETWORK SECURITY 5
DATA SECURITY 6
FIREWALLS 6
ENCRYPTION 7
SSL Encryption 7
Public Key Infrastructure (PKI) (Optional) 7
Database Encryption (Optional) 7
DISASTER RECOVERY 7
BASIC DISASTER RECOVERY PLAN 7
PREMIUM DISASTER RECOVERY PLAN (OPTIONAL) 8
HIPAA COMPLIANCE 9
UNAUTHORIZED ACCESS 9

BOWMAN systems

SECURING CLIENT DATA

Bowman Systems is committed to maintaining optimum client data security by meeting and exceeding industry standard practices. As a leader in software and Information Technology (IT) services for the health and human services industry, Bowman Systems considers data security as the cornerstone of all of its development efforts. In 1999, Bowman Systems pioneered its secured data-sharing model, enabling multi-agency collaboratives to collaborate while safeguarding client data (*ServicePoint* 1.0). In 2000, Bowman Systems was the first web-based client data system to offer integrated database-level encryption. Again, in 2001, Bowman Systems pioneered its integrated Audit Trail system before the HIPAA requirement.

Bowman Systems has always held conviction that our products be fully web based and that we own and operate our own data center. We seek to provide best of class data center services to ensure data security and regulatory compliance, and continuously expand and invest in our data center to include physical security, network security, redundant power, redundant HVAC, fire suppression systems and full time staff to manage all of the afore mentioned.

This document outlines the measures taken by Bowman Systems to secure all client data on each of our customer's *ServicePoint* sites. The steps and precautions taken to ensure that data is stored and transmitted securely are divided into six main sections – Access Security, Site Security, Network Security, Disaster Recovery, HIPAA Compliance, and Unauthorized Access.

ACCESS SECURITY

Access Security begins at Bowman Systems with a focus on the following areas:

- Bowman Systems Employees
- Bowman Systems Access to *ServicePoint*
- Audit Trails
- Customer Access to *ServicePoint*.

Bowman Systems Employees

Bowman Systems' designated Security Officer assures employees are held to the highest standards when it comes to both company and customer data security. Employees who have access to client data are subject to a national background check, training on confidentiality requirements (company, HIPAA, HUD), and must sign a confidentiality statement as part of their employee agreement.

Bowman Systems Access to ServicePoint

- Only a limited number of Bowman Systems' staff has access to a customer's *ServicePoint* site and client data. Access occurs only when you request an installation, import of data, implementation upgrade, or require assistance by support staff to troubleshoot a problem.

BOWMAN systems

- The contract between the customer and Bowman Systems legally compels Bowman Systems to hold all client data stored in the customer's database in strict confidence. Bowman Systems will take all reasonable precautions to prevent the disclosure to outside parties of such information, except as may be necessary by reason of legal, accounting or regulatory requirements.
- Access to the customer's system data by Bowman Systems support staff can be monitored by running an *Audit Report* (see Automated Audit Trail below).

Audit Trail

- *ServicePoint* automatically tracks caller, client, and resource related activity by the use of an audit trail. This system function logs the time and type of activity, as well as the name of the user who viewed, added, edited, or deleted the information.
- All changes to Resource records are automatically tracked by the User (updates, as well as, date and time the updates were made). In addition, there is a Date of Official Update that is set when the Resource record has been formally reviewed. This section includes not only date and time of the Official update but also which User performed the action, which organization requested the Official Update, and a notes field for describing the reason for the update (such as Annual Review, Agency Request, etc).
- • To retrieve information created by the audit trail, an *Audit* report can be generated in the Reporting section of *ServicePoint*. Access to client audit information is limited to System Administrator and Agency Administrator access levels.

Customer Access to ServicePoint

- To ensure authorized access, each user is issued a user name and password for entrance into the *ServicePoint* application.
  - Each *ServicePoint* user is required to have a unique User ID to log into the application.
  - Passwords must be 8 to 16 characters in length and must contain at least two numbers.
  - The system allows only one login per password at a time. A user cannot log into the system on two terminals at the same time using a single password.
  - Passwords automatically expire every 45 days requiring the user to create a new password.
  - A prompt appears when you need to choose a new password.
  - The same password cannot be used consecutively.
  - To enforce password security, *ServicePoint* will not allow a browser to save a password. In addition, if FOUR consecutive logon attempts with the incorrect password are made the user account will need to be reset by your System Administrator. This security feature prevents access to the site by a password generator.
  - Passwords are stored as hashed values in the *ServicePoint* database
- *ServicePoint* has an automatic logout function for users who have been idle for a pre-determined period. (The default setting is 30 minutes.) This function decreases potential viewing and/or manipulation of client data by unauthorized individuals. Although the default setting is 30

minutes, each installation can request Bowman Systems to set the system timeout for a length that meets their particular policies and procedures.

- To limit who can view and/or modify the customer's client data, individuals are assigned one of sixteen (16) User Access Levels. Each user level has certain security restrictions applied to it. Each user level has access to certain *ServicePoint* features and the ability to view certain pieces of client information. The System Administrators II can see all data, even when it is closed.
  - Each level grants different access rights to the various sections (ClientPoint, ResourcePoint, SkanPoint, ShelterPoint, Admin etc.) of the application.

SITE SECURITY

Site security is a high priority since it not only helps protect the customer's stored client data, but also protects the equipment used to host the customer's data. To ensure the protection and service reliability for the customer's system, Bowman Systems has instituted the following security levels:

Building Security

Bowman Systems' offices are located in a large commercial complex with the following perimeter security systems:

- 24-hour security personnel
- 24-hour video surveillance
- Building fire suppression system
- After-hours Key Card entry to building
- After-hours Key Card elevator access
- Locked stairwells during non-business hours.

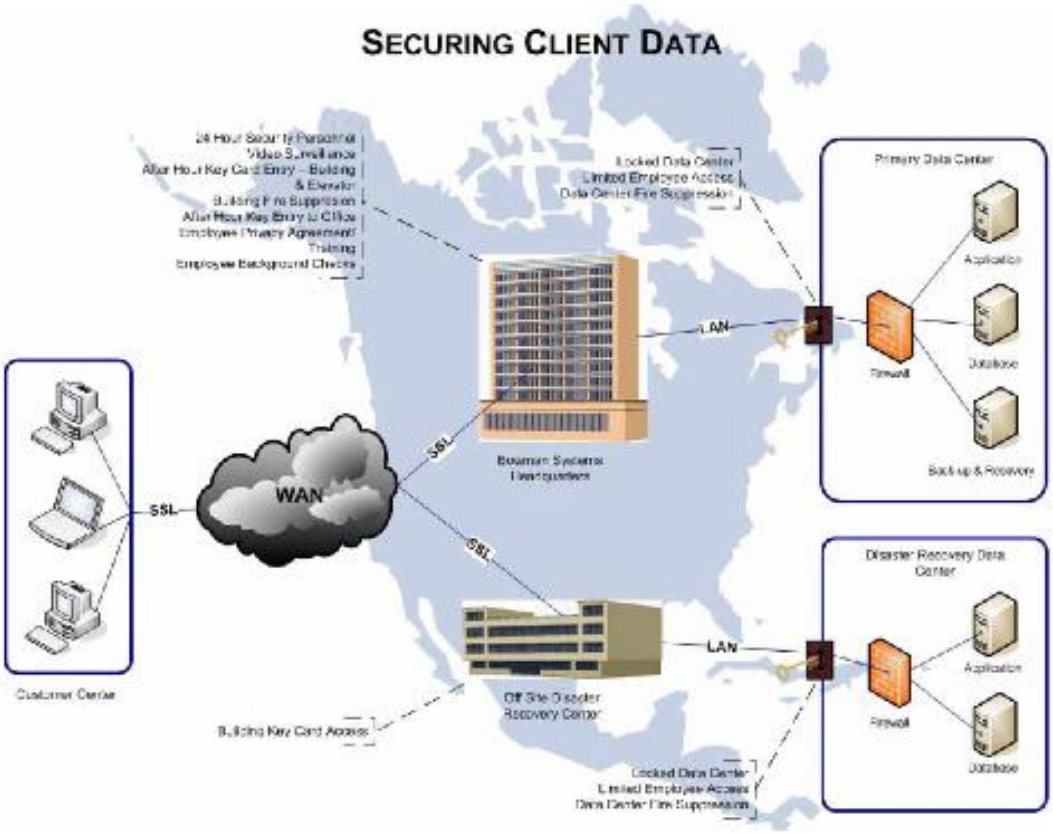
Bowman Systems Headquarters Security

The Bowman Systems offices and data centers include the following additional levels of security.

- After-hours key entry to offices
- Dedicated and secured Data Center
  - Locked down 24-hours per day
  - Two separate, fully redundant HVAC systems for server areas
  - Only accessible by management controlled key
  - Protected by a state of the art, non-liquid automatic fire suppression system
  - No access is permitted to the office cleaning staff

BOWMAN systems

- Accessed by key personnel only (e.g. Information Technology and Management staff). Access is required for nightly data backups, new installations, upgrades and maintenance.



NETWORK SECURITY

Database security includes protection of client data residing on the database server and as it is transmitted over the internet through the application server. The security measures in place ensure that client data is only available and accessed by authorized users.

There is a nightly backup of the *ServicePoint* system that is comprised of a backup of the database and a backup of the application code. Our standard protocol includes nightly tape backup of the client's database that is carried three miles off-site and stored in a fireproof facility. Bowman Systems maintains redundant power for all on-site servers via building power and building generator and redundant bandwidth provided via two separate upstream providers. Our data center contains a state-of-the-art, non-destructive fire-suppression system. Bowman Systems also utilizes RAID 5 (Redundant Array of Independent Disks) to mirror the hard drives, provide faster data throughput and ensure reliable data.

BOWMAN systems

- Multiple broadband connections, fully load balanced for reliability and speed.
- Reliable Enterprise class Cisco switches and routing equipment.
- A natural gas powered generator capable of powering the facility indefinitely and UPS backups to supply uninterrupted power. This system is tested monthly (in such a way that power is not interrupted) to ensure reliability.
- Two separate, fully redundant HVAC systems for server areas.
- A non-liquid automatic fire control system.
- A physically secure building with keycard access, video surveillance and 24 x 7 security guard controlled access.

Data Security

To ensure availability of customer data in the event of system failure or malicious access, redundant records are created and stored in the following manner:

- Nightly database backups.
- Offsite storage of backups
- 7 day backup history stored locally on instantly accessible RAID storage
- 24 hours backed up locally on instantly-accessible disk storage
- 1 month backup history stored off site
- 24 x 7 access to Bowman Systems emergency line to provide assistance related to "outages" or "downtime".

Firewalls

To enhance security further, firewalls are in place on all servers hosted by Bowman Systems. As detailed below, there are multiple levels of firewall security:

- The *ServicePoint* application and database servers are separate from the Bowman Systems internal network.
- Bowman Systems utilizes an industry standard Intrusion Detection System to pinpoint unauthorized attempts at accessing its network and to shield the customer's data in the event of such an attempt.
- Only regular and secured HTTP traffic are permitted through to the Bowman Systems application servers.
- As a security policy, specifics on the type of equipment, protocols, and procedures in use are never revealed.
- Database servers are only accessible via an internal network connection from our application servers.

BOWMAN systems

Encryption

SSL Encryption

SSL encryption ONLY encrypts the data going across the internet to the end-user's web browser. Bowman Systems uses AES-256 encryption (Advanced Encryption Standard, 256-bit) in conjunction with RSA 2048-bit key lengths. A description can be found at http://en.wikipedia.org/wiki/Key_size.

When an end-user accesses their site, an SSL (encrypted) negotiation is performed between the server at Bowman Systems datacenter and the end user's web browser. The traffic that then flows between the server and the end user's workstation is encrypted using the SSL certificate installed on that server. This prevents anyone that is sitting in between our server here and the end user's workstation from being able to intercept potentially sensitive data. The AES-256 is the method in which the data is encrypted. There are various forms of SSL encryption. The key length make it more difficult to decrypt the encrypted data.

PUBLIC KEY INFRASTRUCTURE (PKI) (OPTIONAL)

As an option, Private Key Infrastructure (PKI) is available for those needing additional security frameworks. PKI is an additional layer of security on TOP of our standard SSL certificates. It is still SSL encrypted, however, this method of encryption requires a matching server certificate / client certificate pair in order to unencrypt the data that is sent from the end user's *Servicepoint* site to their Web Browser. Without the appropriate PKI client certificate installed on the end-user's workstation, their web browser will not be able to unencrypt the data and therefore will not be able to access the site. The PKI Client Certificate cannot be installed on a workstation without the appropriate password that accompanies the certificate. This allows the customer to regulate exactly who can and who cannot access their *Servicepoint* site.

Database Encryption (Optional)

The data in *ServicePoint* encrypted databases are encrypted with AES-128.

DISASTER RECOVERY

Due to the nature of technology, unforeseen service outages may occur. In order to assure service reliability for hosted *ServicePoint* applications, Bowman Systems offers the following disaster recovery options.

Basic Disaster Recovery Plan

The basic Disaster Recovery Plan is included in the standard *ServicePoint* contract and includes the following:

- Nightly database backups.
- Offsite storage of backups
- 7 day backup history stored locally on instantly accessible RAID storage

BOWMAN systems

- 1 month backup history stored off site
- 24 x 7 access to Bowman Systems emergency line to provide assistance related to "outages" or "downtime".
- 24 hours backed up locally on instantly-accessible disk storage

Standard Recovery: All customer site databases are stored online, and are readily accessible for approximately 24 hours; backups are kept for approximately one (1) month. Upon recognition of a system failure, a site can be copied to a standby server, and a database can be restored, and site recreated within three (3) to four (4) hours if online backups are accessible. As a rule, a site restoration can be made within six (6) to eight (8) hours. On-site backups are made once daily and a restore of this backup may incur some data loss between when the backup was made and when the system failure occurred.

All internal servers are configured in hot-swappable hard drive RAID configurations. All systems are configured with hot-swappable redundant power supply units. Our Internet connectivity is comprised of a primary and secondary connection with separate internet service providers to ensure redundancy in the event of an ISP connectivity outage. The primary Core routers are configured with redundant power supplies, and are configured in tandem so that if one core router fails the secondary router will continue operation with little to no interruption in service. All servers, network devices, and related hardware are powered via APC Battery Backup units that in turn are all connected to electrical circuits that are connected to a building generator.

All client data is backed-up online and stored on a central file server repository for 24 hours. Each night a encrypted backup is made of these client databases and secured in an offsite datacenter.

Historical data can be restored from backups as long as the data requested is 30 days or newer. As a rule, the data can be restored to a standby server within 6-8 hours without affecting the current live site. Data can then be selectively queried and/or restored to the live site.

For power outage, our systems are backed up via APC battery back-up units, which are also in turn connected via generator-backed up electrical circuits. For a system crash, Non-Premium Disaster Recovery Customers can expect six (6) to eight (8) hours before a system restore with potential for some small data loss (data that was entered between the last backup and when the failure occurred) if a restore is necessary. If the failure is not hard drive related these times will possibly be much less since the drives themselves can be repopulated into a standby server.

All major outages are immediately brought to the attention of executive management. Bowman Systems support staff helps manage communication or messaging to customers as progress is made to address the service outage. Bowman Systems takes major outages seriously, understands, and appreciates that the customer becomes a tool and utility for daily activity and client service workflow.

Premium Disaster Recovery Plan (Optional)

The *optional* Premium Disaster Recovery plan includes all of the Basic Plan features plus several additional levels of support to enhance disaster recovery capability. Additional features included are as follows:

- Off site on a different Internet provider and on a separate electrical grid backups of the application server via a secured Virtual Private Network (VPN) connection

BOWMAN systems

- Near-Instantaneous backups of application site (no files older than 15 minutes)
- Minute-level off site replication of database in case of a primary data center failure
- Priority level response (ensures downtime will not exceed 4 hours)

HIPAA COMPLIANCE

HIPAA compliance is a requirement for many agencies that use *ServicePoint*, particularly as the compliance relates to the HIPAA standards for security. The following five (5) methods ensure that *ServicePoint* is fully compliant with HIPAA data center standards:

- Network Security includes firewalls, certification servers, VPN access, and Operating System authentication.
- Encryption (optional – pricing is available upon request) is a database level security which encrypts confidential information located in the database tables.
- Audit Trails log and report on users who have viewed, updated, or deleted client records.
- Client Record Privacy Options allow or restrict access to all or part of a client file, including individual fields (data level).
- Automatic timeout logs a user out of the system after a specified period, thereby decreasing the potential viewing or manipulation of client data by unauthorized individuals.

UNAUTHORIZED ACCESS

If an unauthorized entity were to gain access to a customer's system and client data or if there were suspicion of probable access, Bowman Systems would take the following steps:

- The system would be examined to determine the presence of system or data corruption.
- If the system has been compromised, the system would be taken offline.
- Using the previous night's backup, a restored copy of the system data would be loaded onto another server, and the system brought back on line with the back-up data.
- Comparing the back-up database to the database taken offline, an investigation would be launched to determine the extent of the unauthorized activity/corruption, and the corrective action needed.
- Upon completion of the investigation, findings would be reported to the customer and options would be discussed.
- Upon customer approval, corrective action would be initiated. Corrective action could include all or part of the following:
  - The original hard drive would be completely erased and rebuilt, including a new operating system, SSL Certificate, application(s), and the back-up database.
  - If applicable and feasible, lost data from the original database would be restored.

ATTACHMENT E – Maricopa HMIS Data Quality Plan

MARICOPA HMIS PROJECT

DATA QUALITY AND MONTORING PLAN

Maricopa HMIS Project Document
Approved by the Maricopa Continuum of Care Regional Committee on Homelessness on March 18, 2013

The Maricopa Homeless Management Information System (HMIS) is a program funded by the U.S. Department of Housing and Urban Development (HUD) and managed by Community Information and Referral Services (CIR). The Maricopa HMIS Project is designated to CIR by the Maricopa Regional Continuum of Care Regional Committee on Homelessness (CoC).

Definition of Data Quality

HMIS data quality refers to the extent that data recorded in an HMIS accurately reflects the same information in the real world. However, to meet the HMIS goal of presenting accurate and consistent information on homelessness, it is critical that an HMIS have the best possible representation of reality as it relates to homeless people and the programs that serve them. Specifically, it should be our goal to record the most accurate, consistent and timely information in order to draw reasonable conclusions about the extent of homelessness and the impact of homeless services.

Enhancing HMIS Data Quality July 2005

U.S. Department of Housing and Urban Development

Office of Community Planning and Development

Importance of Data Quality for HMIS Goals

"There has never been an overall review or comprehensive analysis on the extent of homelessness or how to address it. The Committee believes that it is essential to develop an unduplicated count of homeless people and an analysis of their patterns of use of assistance …including how they enter and exit the homeless assistance system and the effectiveness of assistance." *2001 Congressional Directive*

These goals are not only important on the federal level but also critical for understanding homelessness and program planning at the local level.

Pattern of Homeless Service Utilization

People who are homeless often use more than one of the programs that are available to help them access housing, resolve their crisis, support them, and link them with other services. Accurate program entry and exit dates and information on residence prior to program entry are critical in determining service use patterns that assess average length of stay and movement among different homeless programs. The collection of accurate identifying information at each program is also necessary in order to identify the extent to which clients appear in multiple programs, how clients move through the system, and to detect cycles of homelessness.

Effectiveness of the Homeless Service System

Assessing the effectiveness of the current homeless service system is critical to finding successful solutions to ending homelessness. For that reason, information at program exit, such as destination and income, are

important to learn if and how the system has helped to resolve clients' housing crisis and to improve their overall stability. Data on returning clients also contribute to this goal. Comparing program entry data with program exit data at the aggregate level will also provide a picture of homeless program impacts on the clients they serve.

I. Data Quality Plan

A. Data Quality Benchmarks

As stated in the 2009 HMIS Data Quality Standards issued by HUD, all contributory Homeless Assistance programs need to follow HUD determined data quality benchmarks. These benchmarks are determined by HUD and are required for all Continuums throughout the nation. The goal of the benchmarks is to attain consistent data from all Continuums. The benchmarks in the following areas have been determined.

1. Timeliness of Data

To be most useful for reporting, an HMIS database should include the most current information on the clients served by participating homeless programs. To ensure the most up to date data, information should be entered as soon as it is collected. All Client data will be entered by the fifth day after occurrence.

a. Client information is entered within 5 days following the occurrence in which the client was served

b. Client information is updated regularly at exit or annual assessment – per requirements relative to each universal and program specific data elements.

2. Data Accuracy

Information entered into the HMIS database needs to be valid and accurately represent information on the people that enter any of the programs contributing data to the HMIS database. Inaccurate data may be intentional or unintentional. In general, false or inaccurate information is worse than incomplete information, since with the latter, it is at least possible to acknowledge the gap. Thus, it should be emphasized to clients and staff that it is better to enter nothing (or preferably "don't know" or "refused") than to enter inaccurate information.

a. 95% of data entered into the HMIS database must reflect what clients are reporting

b. Staff entering information into the HMIS database must enter information as stated by the client. Every program must enter data on clients in the same way over time, regardless of which staff person is recording the data in HMIS.

3. Data Completeness

For accurate reporting purposes by the Maricopa HMIS Project, data needs to be as complete as possible, and should contain all required information on all clients served in a program during a specified time period. The goal of achieving HUD defined required HMIS coverage and participation by all local programs is essential for ensuring that the records are representative of all the clients served by these programs.

a. 100% of all HUD funded homeless assistance programs in Maricopa County must participate in the Maricopa HMIS Project

b. 100% of all clients entered will have complete HUD Universal Data Elements

c. 98% of clients will have complete program data elements entered

d. 98% will have services entered, if services are required

e. 98% of clients that exit will have data entered with exit destinations

f. 10% is the maximum allowance for null or missing data

g. 5% is the maximum allowance for “don’t know” and “refused” responses of all answered questions

h. 75% of all beds in non-HUD funded residential homeless assistance programs located in Maricopa County must participate in the Maricopa HMIS Project

4. Training

Standardized training is provided by the Maricopa HMIS Project and is vital to attaining quality data entry. Software training is performed using a standardized curriculum, presented in a consistent manner by the Maricopa HMIS Project team.

a. User training will cover how to collect data, how to pass data from front-line staff to data entry staff, how to log questions about the data and how to resolve those questions, how to give feedback, and expectations for participating in user meetings. Some of these issues may be program specific, so they may need to be addressed by custom or specialized training rather than as part of the system-wide software training.

b. All users must attend a minimum of one training session annually.

B. Consistency Among Agencies

The Maricopa HMIS Project staff should ensure consistent data collection and quality across all of its participating programs. This can be achieved through some or all of the following mechanisms.

1. Continue HMIS Data Quality Group

   The Data Quality Group is charged with making sure data quality remains prominent in CoC decision-making. Any recommendations will be reported by this group to the HMIS User Group.

2. Continue HMIS User Group meetings

   The HMIS User Group meetings keep HMIS users abreast of HMIS efforts across the CoC. This helps maintain momentum, identify user concerns and software needs, share solutions to common problems and best practices, and provides opportunities to review and refine data quality processes.

3. Continue HMIS Advisory Board meetings:

   The HMIS Advisory Board advises and supports the Maricopa HMIS Project and CoC's operations. The HMIS Advisory Board makes final approval of all recommendations to be brought to the CoC.

4. Conduct routine analyses/comparisons between programs:

   Comparisons among CoC programs can serve as a healthy competition to meet the standards set by the CoC and can also serve to identify best practices in data quality and general usage.

5. Define parameters for data definitions:

   The HMIS User Group is uniquely positioned to ensure common parameters (or meaning) to questions in the HMIS database. For example, is asthma a physical disability? Is PTSD a mental illness or a separate category? If there is confusion around questions that the Maricopa HMIS Project Team or software documentation cannot answer easily, the Data Quality Group can discuss and agree upon a convention. This information should be shared throughout the CoC (and also with the software provider).

6. Monthly and/or Quarterly reports will be generated from the HMIS database to verify timely data entry and quality assurance:

   Quarterly reports to the Advisory Board and to the CoC are a way to strengthen agencies compliance and promote a culture where data collection and quality is taken seriously and completed.

7. Programming queries and generating regular data quality reports:

The Maricopa HMIS Project team can play an important role by providing agencies with standard queries or tools to help them verify their agency's data quality. Similarly, these reports can be run on the overall system data to identify data errors.

8. Institutionalize a feedback loop to agencies:

   The Maricopa HMIS Project team and the Data Quality Group can create a process for all agencies to submit data quality issues in order to remediate discrepancies between program performance and standards. The Data Quality Group can use this information to help the Maricopa HMIS Project assess the quality of data and establish consistency between HMIS participating programs.

II. Monitoring Plan

Information entered into HMIS must be entered in a timely manner. It is required that all information be entered into Maricopa HMIS Project within 5 days of the occurrence. The programs entering information into the Maricopa HMIS Project must update client information at exit from the program or during regular assessment updates. It is important that information is kept up to date in the Maricopa HMIS database for data quality for reporting.

A. Report Utilization

Data Quality reports will be used to assess individual program data quality. The HMIS project team will be responsible for developing Data Quality reports. The individual programs will be able to access the reports relevant to their programs. This will enable each program to monitor their data and improve data quality on an individual basis. It is recommended that each program run data quality reports on a monthly basis to meet the required HUD benchmarks.

B. Implementation Plan

1. Month 1: Goal: Assess Baseline Compliance Rate = 85% of HMIS Participating Agencies Achieve Data Quality Benchmark Compliance

   a. All data entered by providers up to current month

   b. Program data quality reports provided to the HMIS Data Quality Group for initial review

   c. Data quality reports reviewed by the HMIS Data Quality Group

   d. Providers correct data errors in HMIS database

   e. Revised aggregate data quality reports generated and published to the HMIS website

   f. Data quality progress report developed

g. Assess training needs and post training schedule/plan on HMIS website

2. Month 4: Goal: Increase Baseline Compliance Rate = 88%

   a. Initiate Quarterly Compliance Rate Report reviewed by the HMIS Data Quality Group

   b. Initiate Quarterly Compliance Rate Report will be posted to the HMIS website

3. Month 7: Goal: Increase Baseline Compliance Rate = 90%

4. Month 10: Goal: Increase Baseline Compliance Rate = 92%

5. Month 12: Goal: Increase Baseline Compliance Rate = 95%

   a. Annual Compliance Rate Report reviewed by the HMIS Data Quality Group and submitted to and approved by the HMIS Advisory Board

   b. Annual Compliance Rate Report will be posted to the HMIS website

   c. Compliance Rate Report will be posted to the HMIS website

   d. Presentation of data quality progress report at general CoC meeting – Annually

   e. When a 95% compliance rate is achieved, the goal will be to achieve 98% compliance rate for all data entered in HMIS

C. Reporting Requirements

HUD is requiring as part of the HUD data standards specific reports for data quality. Maricopa HMIS will produce the reports as required by HUD. These reports will change as HUD's regulations change.

1. The first report is a null/missing values report. These reports show what percentages of fields are left blank or marked "don't know" or "refused." It compares those numbers to the potential number if all client records had all required fields complete. The report will show the amount of null/missing information in the HMIS database. This report can reflect the null or missing values for different program types across the CoC.

2. The second required report is an unduplicated data quality report. This report helps determine if clients are entered into the HMIS database more than once. To achieve high quality data, it is important that there is only one record per client. If a client is counted multiple times the information in the report will be incorrect.

3. A bed utilization report is required showing the percentage of beds or units filled on any given night. This report can show HUD and the CoC how the Maricopa HMIS Project programs are using their beds.

The bed utilization report will also show programs that are reporting an overutilization or underutilization of beds. For example, an agency that shows a repetitive 105% or higher occupancy rate, or an agency that shows a 60% or lower occupancy rate, would present an inconsistent bed utilization.

4. A timeliness report is required to monitor the data timeliness benchmark. This report will show that data is being entered in a timely manner. It will also show differences in dates. For example, the timeliness report will show the gap in time between when the client entered the program and the date that the data was entered into the HMIS database.

D. Programs will comply with HUD Data Standards including Program Elements, Universal Data Elements, Self-Sufficiency Matrix and User Training as stated in the CoC Program Performance Report.

E. As required in the HEARTH ACT, the Maricopa HMIS Project will work in conjunction with the CoC to ensure data coverage to meet the minimum bed coverage rates and service volume coverage rates as established by HUD.

F. Maricopa HMIS Project programs are subject to site visits from the Project team to ensure overall HMIS compliance.

HMIS Data Quality Depth of Data Elements

Name:

- First and Last Name not the same
- Suffix properly formatted
- No numerals in name fields (except Suffix)
- Suffixes not in last name field
- First name is not “Husband”; ”Wife”; ”Woman”; ”Man”; ”Baby” ;”Girl” ;”Boy” of similar

Social Security Number/Quality Code:

- SSN has all numbers and no dashes
- 9 digits when quality code indicates complete
- Less than 9 digits when quality code indicates partial
- All digits not the same; all numbers not sequential (123456789)

Date of Birth:

- Earlier than current date
- Earlier than program entry date
- Later than 90 years from present
- Not minor in Adult shelter/Adult in youth shelter

Ethnicity/Race:

- Primary and secondary race not the same

Gender:

- Men not pregnant
- No male in woman’s shelter/woman in men’s shelter

Veteran Status:

- Client under 18 not veteran
- All veterans in veteran shelter
- Those receiving veteran’s pension marked as veteran

Disabling Condition:

- Those receiving SSDI for themselves are marked as having a disability
- Those indicating substance abuse, mental health, physical disability, developmental disability, HIV/AIDS marked as having disability

Residence prior to program entry

- Self-report not contradicted by other HMIS data

Zip Code of Last Permanent Address/Quality Code

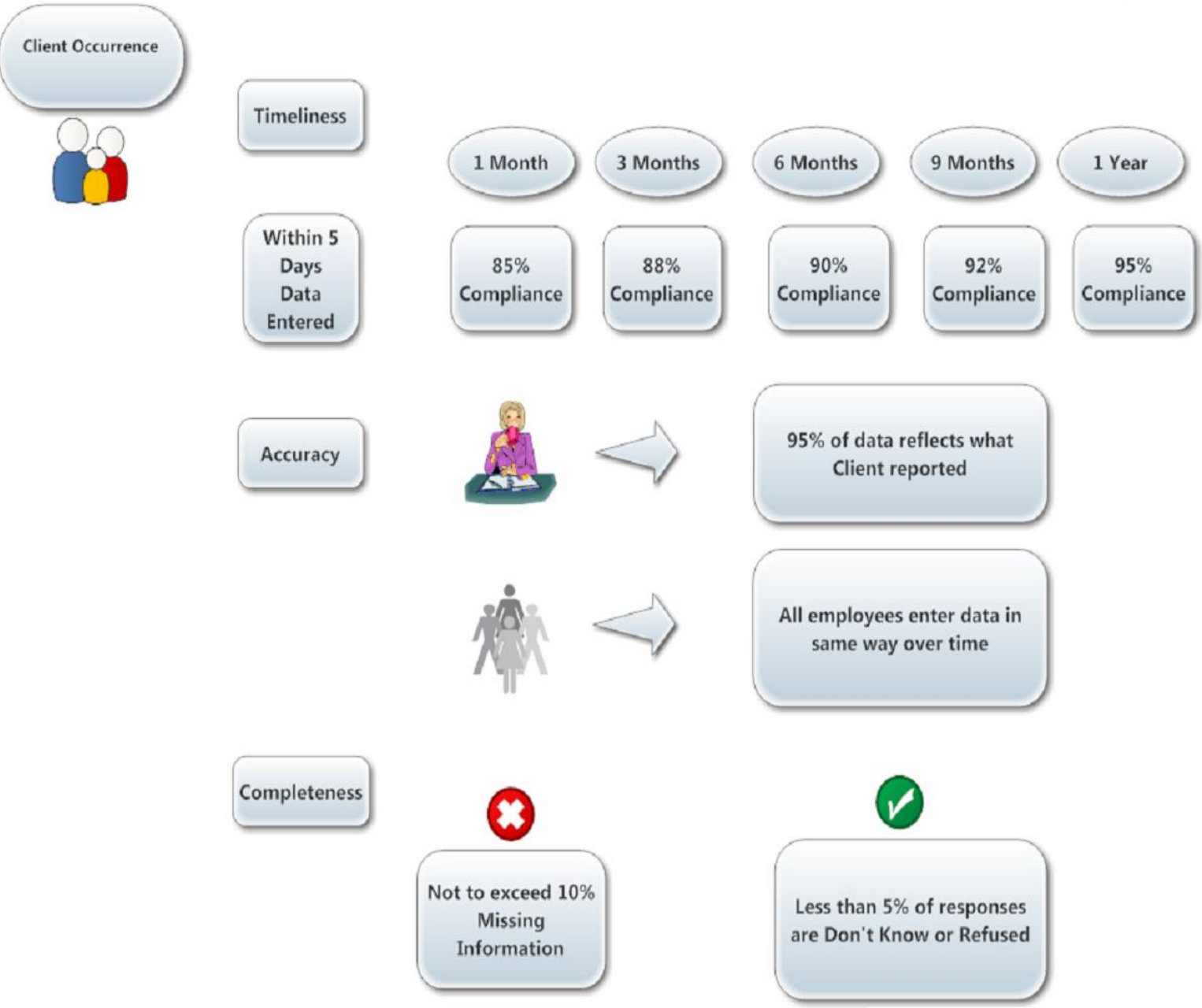
- Zip code complete if quality code marked as complete
- Zip code five or nine characters
- Zip code is valid
- Zip code has only numbers

Program Entry Date/ Program Exit Date

- All clients have a program entry date
- Program entry date later than birth date
- Program entry date prior to Exit date
- Entry and exit date not the same in residential shelter
- Length of program enrollment outliers are reasonable considering program type

Household ID

- No single person in family shelter
- No family in individual shelter
- One Head of Household per family


Client Occurrence
Timeliness
1 Month
3 Months
6 Months
9 Months
1 Year
Within 5 Days Data Entered
85% Compliance
88% Compliance
90% Compliance
92% Compliance
95% Compliance
Accuracy
95% of data reflects what Client reported
All employees enter data in same way over time
Completeness
Not to exceed 10% Missing Information
Less than 5% of responses are Don't Know or Refused

ATTACHMENT F – Maricopa HMIS Privacy Notice

Privacy Notice

Effective xx/xx/2016

Version 1.0

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

A. What This Notice Covers

1. This notice describes the privacy policy and practices of [Name of Agency]. Our main office is at [Address, web address, telephone contact information.]2. If this agency operates programs which are covered by HIPAA laws, additional privacy information will be provided and supersedes information in this Privacy Notice.

3. Our agency and many others participate in the Maricopa Regional Continuum of Care (CoC). The CoC promotes and funds communitywide goals and programs to end homelessness and utilizes data to make informed decisions.

4. The Maricopa Regional CoC has approved the use of various data systems for the collection and sharing of personal information including a computer system called a Homeless Management Information System (HMIS) and Homelink a software program utilized for matching clients to appropriate housing interventions. The CoC may approve additional data systems for community use in the future.

5. When a person requests or receives services from this agency or other agencies participating in the CoC, information about them and members of their household will be entered into these computer systems. These computer systems will be used by multiple agencies.

6. The policy and practices in this notice cover the processing of Protected Personal Information (PPI) of this and other agencies utilizing the approved data systems of the CoC. All personal information that the agencies maintain, not just the information entered into the data system, is covered by the policy and practices described in this notice. This policy covers only the programs within the agency that participate in HMIS.

7. Protected Personal Information (PPI) is any information we maintain about a client that:

a. allows identification of an individual directly or indirectly

b. can be manipulated by a reasonably foreseeable method to identify a specific individual, or

c. can be linked with other available information to identify a specific client. When this notice refers to personal information, it means PPI.

8. We adopted this policy to provide accurate information about how your data may be used and to comply with the privacy standards for Homeless Management Information Systems (HMIS) and all CoC approved databases.

We intend this policy and practices to be consistent with the standards of 69 Federal Register 45888 (July 30, 2004).

9. This notice tells our clients, our staff, and others (such as our funders, the CoC and other social services providers) how we process personal information. We follow the policy and practices described in this notice.

10. We may amend this notice and change our policy or practices at any time. Amendments may affect personal information that we obtained before the effective date of the amendment. All amendments are approved by the CoC Board. Current information about the CoC Board can be found at the MAG website www.azmag.gov/Committees/.

11. We give a written copy of this privacy notice to any individual who asks. We maintain a copy of this policy on the MAG website at www.azmag.gov.

12. The HMIS is administered by Community Information and Referral (CIR). Their office is at 2200 N Central Ave Ste. 211; Phoenix, AZ, 85004. Their website is www.211arizona.org. You can contact the system administrator at 602-263-8845.

13. Homelink is administered by the Human Services Campus/Lodestar Day Resource Center located at 234 S 12th Ave; Phoenix, AZ, 85007. You may contact the system administrator at 602-759-5356.

14. The agency to contact regarding the CoC is the Maricopa Association of Governments located at 302 N. 1st Avenue, Phoenix, AZ 82003. Their phone number is 602-254-6300.

B. How and Why We Collect Protected Personal Information

1. We collect personal information only when appropriate to provide services or for another specific purpose of our agency or when required by law.

2. We may collect personal information for these purposes:

a. To provide or coordinate services to clients

b. To locate other programs that may be able to assist clients

c. To verify information given to us by clients

d. For functions related to payment or reimbursement from other services that we provide

e. To operate our agency, including administrative functions such as legal, audits, personnel, oversight, and management functions

f. To comply with reporting obligations

g. To improve services on a system level

h. When required by law

3. We may be required to collect some personal information by law or by organizations that give us money to operate this program. Other personal information that we collect is important to run our programs, to improve services, and to better understand the needs of individuals in the community. We only collect information necessary to coordinate and deliver services.

4. We only use lawful and fair means to collect personal information.

5. We collect personal information with your knowledge and consent. If you seek our assistance and provide us with personal information, we verify your consent to the collection and processing of that information as described in this notice.

6. We may also get personal information, with your consent, from:

a. Individuals who are you have identified as part of your household

b. Individuals who you have identified as assisting you

c. Individuals or organizations you provide for verification of information or references

d. Information already collected about you by other agencies that are part of the HMIS

e. Other private organizations in the CoC

f. Government agencies and their data systems including Regional Behavioral Health Authority

g. Public records including internet searches, telephone directories and other published sources

7. We post a sign at our intake desk or other location explaining the reasons we ask for personal information. The sign gives our agency's contact information and the location of this privacy notice.

C. How We Use and Disclose Protected Personal Information

1. We use or disclose PPI for activities described in this part of the notice. We may or may not make any of these uses or disclosures with your information. We share client records with other agencies that may have separate privacy policies and that may allow different uses and disclosures of the information.

2. All participating agencies of the CoC share personal client information. The information that is shared with participating agencies may include all information you have provided or has been obtained with your consent. The list of these agencies and the information shared is subject to change. You will be asked to sign a Release of Information to disclose your PPI upon consent. Release of Information document provides specific details of how your information will be shared in the CoC data systems.

3. Agencies use and disclose data pertinent to the services and data collection requirements. Each agency must execute a partnership agreement with the administrator of the data system outlining proper use of the system. All users of the system are required to abide by a code of ethics.

4. You have the right to opt-out of having information shared with other participating agencies and still receive services from that agency. If you opt-out of sharing your information, your information will remain in the data system(s) and be subject to the other disclosures in this privacy notice, but the information will not be available to the other participating agencies. If you opt-out of sharing your information, that decision may change what additional resources or agencies are available to you.

5. By signing the Release of Information, you consent to the use or disclosure of your PPI for the purposes described here:

a. to provide or coordinate services

b. for functions related to payment or reimbursement for services

c. to carry out administrative functions such as legal, audits, personnel, oversight, and management functions

d. to create de-identified (anonymous) information that can be used for research and statistical purposes

e. when required by law to the extent that use or disclosure complies with and is limited to the requirements of the law

f. to avert a serious threat to health or safety if

(1) we believe that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public, and

(2) the use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat

g. to report about an individual we reasonably believe to be a victim of abuse, neglect or domestic violence to a governmental authority (including a social service or protective services agency) authorized by law to receive reports of abuse, neglect or domestic violence

(1) under any of these circumstances:

(a) where the disclosure is required by law and the disclosure complies with and is limited to the requirements of the law

(b) if the individual agrees to the disclosure, or

(c) to the extent that the disclosure is expressly authorized by statute or regulation, and

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

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

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

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

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

h. for academic research purposes

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

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

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

(2) any written research agreement:

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

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

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

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

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

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

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

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

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

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

(c) identifies the PPI sought

(d) is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought, and

(e) states that de-identified information could not be used to accomplish the purpose of the disclosure.

(3) if we believe in good faith that the PPI constitutes evidence of criminal conduct that occurred on our premises

(4) in response to an oral request for the purpose of identifying or locating a suspect, fugitive, material witness or missing person and the PPI disclosed consists only of name, address, date of birth, place of birth, Social Security Number, and distinguishing physical characteristics, or

(5) the official is an authorized federal official seeking PPI for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879 (threats against the President and others), and the information requested is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought.

j. to comply with reporting obligations

k. to the administrators, vendors and contractors of the CoC approved data systems

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

D. How to Inspect and Correct Protected Personal Information

1. You may inspect and have a copy of your PPI that we maintain. We will offer to explain any information that you may not understand.

2. We will consider a request from you for correction of inaccurate or incomplete personal information that we maintain about you. If we agree that the information is inaccurate or incomplete, we may delete it or we may choose to mark it as inaccurate or incomplete and to supplement it with additional or corrected information.

3. To inspect, get a copy of, or ask for correction of your information, ask a program staff member how to obtain this information.

4. We may deny your request for inspection or copying of personal information if:

a. the information was compiled in reasonable anticipation of litigation or comparable proceedings

b. the information is about another individual (other than a health care provider or homeless provider)

c. the information was obtained under a promise or confidentiality (other than a promise from a health care provider or homeless provider) and if the disclosure would reveal the source of the information, or

d. disclosure of the information would be reasonably likely to endanger the life or physical safety of any individual.

5. If we deny a request for access or correction, we will explain the reason for the denial. We will also include, as part of the personal information that we maintain, documentation of the request and the reason for the denial.

6. We may reject repeated or harassing requests for access or correction.

E. Data Quality

1. We seek to maintain only personal information that is accurate, complete, and timely.

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

3. We may keep information for a longer period if required to do so by statute, regulation, contract, or other requirement.

F. Complaints and Accountability

1. Questions or complaints pertaining to the agency serving you should follow the agency's grievance procedure. Questions or complaints that are broader than the services of a single agency or the use of a single data system can be directed to the CoC. If you are unsure where to go, you may go to any agency listed below and we will help you determine the best person to speak with.

[Name of Agency].

[Address, web address, telephone contact information.]

Community Information and Referral (CIR)

2200 N Central Ave Ste. 211

Phoenix, AZ, 85004

www.211arizona.org

602-908-3605

Human Services Campus/Lodestar Day Resource Center

234 S 12th Ave

Phoenix, AZ, 85007

602-759-5356

Maricopa Association of Governments

302 N. 1st Avenue

Phoenix, AZ 82003

602-254-6300

2. All members of our staff (including employees, volunteers, affiliates, contractors and associates) with access to personal information are required to comply with this privacy notice. Each staff member must receive and acknowledge receipt of a copy of this privacy notice.

G. Change History:

1. Version 1.0 April, 2016 – Adopted HUD's baseline privacy notice and approved by the CoC Board.

ATTACHMENT G

Maricopa County HMIS Security Plan

HMIS SECURITY PLAN

The goal of the HMIS Security Plan is to ensure that HMIS data is collected, used, and maintained in a confidential and secure environment at all times. The HMIS Security Plan applies to Community Information and Referral Services (CIR) as the HMIS Lead Agency and System Administrator, HMIS participating agencies, and the HMIS Bowman Systems software. These standards apply to all client information that is collected in the HMIS.

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

HMIS SOFTWARE PROVIDER

The Maricopa HMIS Project uses Bowman System's ServicePoint software. ServicePoint is supported by the most powerful system security measures available. Using 128-bit encryption, user authentication, PKI (Public Key Infrastructure), and user access levels, ServicePoint ensures that data is protected from intrusion.

Bowman Systems' employees, who have access to client-level data, are subject to a national background check, training on confidentiality requirements, and must sign a confidentiality statement as part of their employee agreement. The system function logs the time and type of activity, as well as the name of the user who viewed, added, edited, or deleted the information.

Servers are located in complexes with:

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

LEVELS OF USER ACCESS AND SECURITY

A licensed user is a person who has signed and submitted a Maricopa County HMIS Code of Ethics Agreement and completed basic user training. Provider agencies are required to inform the System Administrator if a user leaves an agency within 24 hours of their termination or departure from the agency. If CIR, as the System Administrator and HMIS Lead Agency, is not notified of their termination

from the agency within twenty-four (24) hours, neither Bowman Systems or CIR as the System Administrator and HMIS Lead Agency will be liable for actions of a former agency employee with an active license.

CIR as the System Administrator will provide each user a unique username and initial password upon completion of training requirements as stated in this manual. CIR will perform an annual user audit for invoicing and licensing purposes. Users are not to share usernames, as this is a breach of the Maricopa County HMIS Code of Ethics agreement and the HMIS Partnership Agreement. Exchanging usernames seriously compromises security and privacy of clients. If a breach occurs, it may subject the agency to discipline and termination of access to the Maricopa County HMIS system. CIR conducts a monthly random audit of users to monitor that users are following the Maricopa HMIS Code of Ethics agreement.

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

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

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

The Bowman Systems software gives agencies the ability to have different user levels. The primary HMIS User types used in Maricopa County are the following (Attachment A):

Read Only II
Case Manager I
Case Manager II
Agency Admin
Executive Director
System Admin II

SECURITY INCIDENT PROCEDURES

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

All HMIS users are obligated to report suspected instances of non-compliance with this policy that may leave HMIS vulnerable to intrusion or compromise client information. The HMIS Lead Agency and System Administrator is responsible for reporting any security incidents involving the real or potential intrusion.

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

If an unauthorized entity were to gain access to the Maricopa County HMIS and client data, or if there is suspicion of probable unauthorized access/activity, CIR as the System Administrator and HMIS Lead Agency, and Bowman Systems will take immediate action to protect the security of the system. Bowman Systems will adhere to the “Securing Client Data” manual (Attachment B).

The system then would be examined to determine the presence of system or data corruption. If the system has been compromised, the system would be taken offline. Using the previous night’s backup, a restored copy of the system data would be loaded onto another server and the system brought back online with the back-up copy. Comparing the back-up database to the database taken offline, an investigation would be launched to determine the extent of the unauthorized activity/corruption and the corrective action needed. Upon completion of the investigation, findings would be reported to CIR and options would be discussed. Upon CIR’s approval, corrective action would be initiated. Corrective action could include all or part of the following:

- The original hard drive would be completely erased and rebuilt, including a new operating system, SSL Certificate, applications and the back-up database.
- If applicable and feasible, lost data from the original database would be restored.

If Bowman Systems or its employees are determined to be at fault for unauthorized access, CIR may terminate the ServicePoint License and Service Agreement and pursue legal remedies.

The HMIS Lead Agency staff will review violations and recommend corrective and disciplinary actions. Each Maricopa HMIS Partner Agency will maintain and follow procedures related to internal reporting of security incidents.

AUDIT AND ACCESS CONTROLS

The HMIS Lead Agency will maintain accessible audit trails that allows for the monitoring of user activity. The HMIS will also authenticate user activity via Internet Protocol address and present simultaneous user access.

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

PERSONAL AUTHENTICATION AND PASSWORD PROTOCOLS

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

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

- All passwords must be unique
- All passwords must be rotated every 45 days
- All passwords must be in a prescribed format recommending a mix of letters/numbers/capitalization/symbols
- Upon the third unsuccessful login try, users will be locked out of the system and the HMIS administrator must reset the password
- All users with no login activity for at least 45 days will be automatically inactivated.

Agency Administrators may reset passwords. If the Agency Administrator is unavailable or otherwise unable to reset a password for an end user, CIR will reset a user's password in the event the password is forgotten. Users must request a password reset by submitting a request to the Maricopa County HMIS Help Desk at HMISsupport@cir.org or by calling the HMIS Help Desk at (602) 908-3605.

CIR will verify the user is active in the system prior to resetting a password. The reset information will be sent back to the user via the Help Desk. The user must enter the password given. The system will only accept this password one time. The system will require the user to create a new password and enter it twice before accessing the database.

PUBLIC ACCESS PROTOCOLS

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

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

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

Examples of allowable Remote Access:

- Personal laptops that were not purchased by the agency.
- Access to the Maricopa County HMIS on a secured private network other than that of the agency.
- Private home desktops.

CIR may audit remote access by Maricopa County HMIS users. If a user is found to have accessed the Maricopa County HMIS through an unsecured network, the user license will be immediately suspended. CIR may impose additional sanctions on the agency including termination of access to the Maricopa County HMIS.

MALWARE AND VIRUS PROTECTION WITH AUTO UPDATE

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

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

DISASTER PROTECTION AND RECOVERY

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

DATA SECURITY AND ENCRYPTION

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

The traffic that flows between the server and the user's workstation is encrypted using the SSL certificate installed on CIR's dedicated servers. Database tape backups are performed nightly. Tape backups are maintained in secure offsite storage. Seven (7) days' backup history is stored on instantly accessible Raid 10 storage. One (1) month's backup history is stored offsite. Users have twenty-four/seven (24/7) access to Bowman Systems emergency line to provide assistance related to outages or downtime.

Attachment A – ServicePoint User Roles

ServicePoint® User Roles Version 5.11 September 5, 2014	Case Manager I	Case Manager II	Read Only II	Agency Admin	Executive Director	System Admin II
ClientPoint						
View client record	X	X	X	X	X	X
View inactive client record						X
Modify client record	X	X		X	X	X
Delete client record				X	X	X
Delete any client record						X
Ability to modify static client security	X	X		X	X	X
Ability to modify dynamic client security	^	^		^	^	X
View client releases of information	X	X	X	X	X	X
Modify / delete client releases of information	X	X		X	X	X
View case managers	X	X	X	X	X	X
Modify / delete case managers	X	X		X	X	X
View Assessments Tab	X	X	X	X	X	X
Add/Edit client answers In Assessment Tab	X	X		X	X	X
View Case Plans Tab	X	X	X	X	X	X
Add/Edit goals, case notes, action steps Case Plans	X	X		X	X	X
View client incidents	X	X	X	X	X	X
Modify / delete client incidents		X		X	X	X
View client needs/services/referrals	X	X	X	X	X	X
Modify / delete client needs/services/referrals	X	X		X	X	X
View client entry/exits	X	X	X	X	X	X
Modify / delete client entry/exits	X	X		X	X	X
View client file attachments	X	X	X	X	X	X
Modify / delete client file attachments	X	X		X	X	X
Delete Households						X
Delete Households (with restrictions)*	X	X		X	X	
ResourcePoint	X	X	X	X	X	X
ShelterPoint	X	X		X	X	X
CommunityPoint						
Global Action given to users in order to disable/hide admin areas which should not be accessible						
CallPoint						
Modify Call Records	X	X		X	X	X
View Call Records	X	X		X	X	X
View Inactive Call Records						X
ActivityPoint						
Add new ActivityPoint Activities	X	X		X	X	X
Edit ActivityPoint Activities	@	@		@	@	X
Delete ActivityPoint Activities	@	@		@	@	X
Manage Activity Attendance in Activity	@	@		@	@	X
Moderate client enrollment into Activities	X	X		X	X	X

Search and View Client Name (Enrollment)	X	X		X	X	X
Assign and manage Activity Volunteer History	X	X		X	X	X
Create new ActivityPoint Volunteers	X	X		X	X	X
Delete ActivityPoint Volunteers				X	X	X
Edit ActivityPoint Volunteers	X	X		X	X	X
Change the user selected as an activity's enrollment moderator				X	X	X
Display/manage only those Activities associated with current user's EDA providers						
Read-only privileges to all ActivityPoint Activities						
By-pass action to grant access to all ActivityPoint data for all providers						X
By-pass action to grant access to all ActivityPoint data for the current user's provider tree				X	X	X
Reports						
Ability to view the reports tab and run reports	X	X	X	X	X	X
Enable the ability to generate system-wide reports						X
Enable ability to delete subordinate or parent provider ReportWriter reports						X
Audit Reports						
Audit Report				X	X	X
User information				X	X	X
User Login				X	X	X
Audit Access Report						X
Provider Reports						
AHAR Report			X	X	X	X
Call Record Report	X	X	X	X	X	X
Client Served Report	X	X	X	X	X	&
Client Intake Report				X	X	X
Daily Unit Report	X	X	X	X	X	X
Duplicate Client Report			X			X
Entry/Exit Report	X	X	X	X	X	&
ESG Caper Report	X	X	X	X	X	&
PATH Report	X	X	X	X	X	&
Referrals Report	X	X	X	X	X	X
Service Transaction Report	X	X	X	X	X	X
Needs Report	X	X	X	X	X	&
Report/Writer	X	X	X	X	X	X
FundManager						
Modify the Provider Preferences controlling FundManager Fund/Vendor creation						X
Full control in the FundManager module						X
Create/modify legacy-style, limited Funds based on the legacy Funding Sources Picklist						X
Access to FundManager module, even if User is not a Review Agent or Fund Administrator				X	X	X
Administration						
Add / edit / delete users				@	@	X
View users				@	@	X

View Inactive Users						X
Reset bad login attempts for users				@	@	X
Reset Passwords				@	@	X
Able to assign resource groups to users				@	@	X
Add Provider						X
Edit Provider				#	#	X
Delete Provider				%	%	X
View inactive providers						X
Modify Provider Visibility information				X	X	X
Modify Provider Services in Provider Admin				X	X	X
Modify Provider Profile information				X	X	X
View Provider Maintenance information				X	X	X
Modify Provider Maintenance information				X	X	X
Add Subordinate Providers				X	X	X
Modify Provider Configuration information				X	X	X
View Provider Configuration information				X	X	X
View Provider Display Settings				X	X	X
Modify Provider Display Settings				X	X	X
Add / edit / remove agency news	X	X		X	X	X
Add / edit / remove system news						X
Access to Create / Read / Update / Delete assessment information. User can change settings						X
Access to AIRS Taxonomy Admin						X
View Picklists						X
Modify Picklists						X
Purchase licenses						X
Allocate and assign licenses				X	X	X
Shadow Mode				X	X	X
View resource groups						X
Add / edit / delete resource groups						X
View reporting groups				X	X	X
Add / edit / delete reporting groups				X	X	X
View visibility groups				X	X	X
Add / edit / delete only local visibility groups				X	X	
Add / edit / delete all visibility groups						X
View EDA groups				X	X	X
Add / edit / delete EDA groups				X	X	X
Send system emails (using Email Admin)				X	X	X
View System Preferences						X
Modify System Preferences						X
Access to Measurements Admin						X
Access to review records in Provider Approval Bin						X
Other						
Export of Providers						X
Provider Admin sections disabled when the provider is outside the current provider's tree						
Bypass Security For the current tree (same as agency-admin bypass in SP v3&4)			X	X	X	

Bypass Security						X
Bypass Release of Info						X
Delete any assessment data system-wide						X
Enter Data As other users	X	X		X	X	
Enable Backdate Mode	^	^		^	^	^
Backdate Release of Info	X	X		X		X
System Support						
Generate XML Exports						X

ATTACHMENT H – Report Request Form

HMIS REPORT REQUEST FORM

Organization Name: _____ Date_____

Contact Information:

Name: _____

Phone Number: _____

E-mail Address: _____

General Information:

Report Name:_____

Purpose of the Report: _____

_____
_____

Project(s) included in the report: _____

_____
_____

Time Period:

From _____ (MM / DD / YY) to _____ (MM / DD / YY)

- ☐ One time only
- ☐ Monthly
- ☐ Quarterly
- ☐ Bi-annual
- ☐ Annual

Requested Completion Date: _____

(Specify the date on which the report is needed)

Report Content:

State in detail what you want in your report. (Write Below or Attach)

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Send request to the following address: HMISsupport@cir.org

ATTACHMENT I – Report Update Form

HMIS REPORT UPDATE OR ISSUE REQUEST FORM

Organization Name: _____ Date_____

Contact Information:

Name: _____

Phone Number: _____

E-mail Address: _____

General Information:

Report Name:_____

Requested Completion Date: _____

(Specify the date on which the report is needed)

Report Content:

State in detail what you updated or what issue you are having with the report. (Write Below or Attach)

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Send request to the following address: HMISsupport@cir.org

ATTACHMENT J – New Project/Project Update Form

HMIS NEW PROJECT/PROJECT UPDATE INFORMATION FORM

Date_____

Organization Name:_____ _____

Contact Information:

Name: _____

Phone Number: _____

E-mail Address: _____

New Project Name (How it will appear in HMIS):_____

_____

Type of Program:

- ☐ HUD Funded CoC
- ☐ HOPWA
- ☐ PATH
- ☐ ESG
- ☐ SSVF
- ☐ RHY
- ☐ Faith Based
- ☐ Other _____

Project Type:

- ☐ Emergency Shelter
- ☐ Transitional Shelter
- ☐ Permanent Supportive Housing
- ☐ Permanent Housing
- ☐ Outreach
- ☐ Rapid Rehousing

- ☐ Homeless Prevention
- ☐ Service Only

Does the project need any of the following ServicePoint resources?

- ☐ Services
- ☐ Referrals
- ☐ ShelterPoint (Bed Tracking)

Please name the Users who will need access to the project:

_____

_____

_____

_____ _____

HMIS Provider Organization Signature Date

_____ _____

CIR Internal Approval Date

Send request to: HMISsupport@cir.org

Guiding Principles of Ranking and Review 2016

To ensure the objective review of resources, maximize HUD funding, and balance community need, the CoC Board and Ranking and Review Panel agree to guiding principles around ranking, review, and reallocation. The CoC Board and Ranking and Review Panel acknowledge that there are insufficient resources for individuals and families experiencing homelessness in the region. The community needs to work to increase capacity for all interventions to meet the need of those experiencing homelessness. For the 2016 NOFA review, cost effectiveness and program performance was paramount in the panel's decisions around funding recommendations.

The group carefully reviewed the scorecards and applications for accuracy, clarity, and consistency with the priorities set forth in the 2016 NOFA. We reached consensus around the following guiding principles:

1) Based on HUD guidance and our funding allocation in the 2015 competition, Transitional Housing resources should be reallocated to Rapid Re-Housing (RRH) or Permanent Supportive Housing (PSH) resources to preserve and possibly increase options keeping the CoC competitive nationally. The group will mirror HUD priorities around Transitional Housing and ensure that we do not lose critical resources in the community.

    a. HUD has clearly indicated that Transitional Housing may be an appropriate intervention for:
       a) underage youth;
       b) victims of domestic violence; and
       c) clients recovering from substance abuse.

2) HUD does not support new Safe Haven programs and has indicated that communities should look carefully at the resource for cost effectiveness and program performance.

3) HUD is urging communities to maximize the use of housing dollars by leveraging support service dollars. The community should move towards financing services through Medicaid funding where possible. Strategic partnerships with MMIC and other community partners will help to transition those projects that receive a majority of CoC-funding for services to seek other sources of funding.

4) The group recommends targeted TA around the following areas:

   - Housing First: Harm Reduction, Motivational Interviewing
   - Project Performance and Evaluation
   - Assistance with transitioning clients in projects that are not recommended for funding to other housing service providers to ensure no returns to homelessness.

5) The community should develop a strategy to increase competition and capacity related to HUD guidance.

TIER 1						
	Agency	Project	Type	Amount	Score	Cost
1	UMOM	RCES MC	SSO	$855,158		
2	CIR	HMIS	HMIS	$400,921		
3	NAC	Camelback	PSH	$816,234		
4	STF	New Direct	RRH	$420,964		
5	NAC	Sunrise Cir	PSH	$35,342	94	$ 1,359
6	Mesa	ARM/STF	PSH	$85,748	93	$ 2,144
7	UMOM	Housing Fir	RRH	$406,373	93	$ 3,945
8	UMOM	Housing Fir	RRH	$272,729	92	$ 3,788
9	ABC	SPC 189	PSH	$1,990,028	92	$ 4,482
10	ABC	SPC 293	PSH	$3,070,558	92	$ 4,798
11	NAC	Catherine A	PSH	$169,721	92	$ 6,286
12	ABC	PSH 3109	PSH	$710,927	92	$ 6,348
13	ABC	HUD 3084	PSH	$963,813	91	$ 5,445
14	US Vets	PERMANEN	PSH	$160,513	90	$ 5,323
16	UMOM	Madison P	PSH	$116,566	89	$ 2,895
17	ABC	SPC 151	PSH	$1,577,126	89	$ 4,369
18	ABC	Village	PSH	$1,856,640	89	$ 5,575
19	ABC	PSH 2009	PSH	$445,823	89	$ 6,557
20	ABC	PSH 3106	PSH	$710,927	89	$ 7,181
21	NAC	Stepping St	PSH	$91,043	88	$ 2,276
22	ABC	HUD 3024	PSH	$531,531	88	$ 7,703
23	Tumblewee	START Hou	PSH	$236,194	88	$ 10,269
24	AHI	Vista Comn	PSH	$40,082	86	$ 2,505
25	ARM/STF	209 West J	PSH	$597,394	86	$ 5,240
26	AHI	Horace Ste	PSH	$60,846	86	$ 6,085
27	AHI	Horace Ste	PSH	$83,429	85	$ 4,391
28	ABC	Casa Mia	PSH	$702,486	85	$ 6,820
29	SBHS	SBHS AIDS	PSH	$22,807	84	$ 1,342
30	ABC	Another Ch	PSH	$1,212,307	84	$ 6,518
31	NAC	Stepping St	PSH	$497,177	84	$ 11,838
32	UMOM	Next Step H	RRH	$694,608	83	$ 1,294
33	ARM/STF	HSC CH-35	PSH	$318,009	83	$ 5,962
34	UMOM	Next Step H	RRH	$329,690	82	$ 2,060
35	Phx Shanti	Shanti	PSH	$72,642	82	$ 4,500
36	ABC	Casa de Lu	PSH	$542,047	82	$ 6,531
37	STF	Homeless F	RRH	$208,566	81	$ 1,862
38	SBHS	Brookside	PSH	$202,663	80	$ 13,511

	Agency	Project	Type	Amount	Score	Cost	
39	CBI	Center for Hope	New Re	$344,610			
40	UMOM	NSH 2 e	New Re	$60,112			
41	UMOM*	Next Step H 3 Realloca	RRH	$434,958			Original bonus project now reallocation from Haven House, AAA, $136,609 of Safe Haven, EVMC
TIER 2							
42	ABC	PSH 2016- Reallocated	PSH	$978,194			Original bonus project now reallocation from Safe Haven
43	Tumblewee	NEW PSH Reallocation	PSH	$257,076			
44	CBI	PSH II-Bonus	PSH	$832,499			
45	US Vets	US Vets PH Proj-Bonus	PSH	$335,806			
46	CBI	CFH-PH	PSH	$184,283	77	$ 8,775	
47	Tumblewee	START Housing Solutio	RRH	$295,096	71	$ 7,975	
48	Tumblewee	START - Housing Soluti	TH	$182,624	68	$ 54,962	partial reallocated to PSH $257,076 & RHY $182,624 held in Tier 2

REALLOCATIONS OR RECOMMENDED NO FUNDING						
Agency	Project	Type	Amount	Sub	Cost	
ANL	East Valley Men's Cent	TH	$58,878	69	$ 3,464	100% reallocated to Next Step 3
Terros	Safe Haven	SH	$1,114,803	78	$ 8,709	100% reallocated; $978,194 to ABC PSH 2016 & $136,609 to NSH 3
ANL	La Mesita-Bonus	PSH	$162,686			Not recommended due to SS only budget, seek Medicaid $
AAA	HIV Case Mngmt/Step	PSH	$37,800	53	$ 2,000	100% reallocated to Next Step 3
CPLC	De Colores	RRH	$322,439			Not recommended due to poor connection with CES
Tumblewee	Start Housing Solution	TH	$439,700	68	$54,962	Reallocated to PSH $257,076 & RHY $182,624 held in Tier 2
UMOM	Haven House	TH	$201,671	85	$ 2,016	100% reallocated to Next Step 3

Membership

The CoC Board membership will be developed and implemented in compliance with requirements from the U.S. Department of Housing and Urban Development (HUD), as defined in the HEARTH Continuum of Care Program Interim Rule released on July 14, 2012. There are three elements within membership including definition of membership structure, selection of members, and ongoing analysis and refinement of membership.

Membership Structure

The first element is defining the membership categories and the number of seats for each category. There will be a minimum of seven seats on the board and a maximum of 13 members. Membership of the CoC Board will follow the agency within the category below, rather than the individual.

Category	Number of Seats (Maximum)
Formerly Homeless Representative	**1**
ESG Recipient's Agency Representative	**1**
Policy/Advocacy Representative	**4**
CoC Funded Provider Representative	**3**
Funder	**2**
Community Seat	**2**

Definition of CoC Board Categories:

- Formerly Homeless Representative: An individual who was at one point homeless.
- Emergency Solutions Grants (ESG) Program Recipient's Agency Representative: HUD defines ESG recipients as state governments, metropolitan cities, urban counties, and U.S. territories that receive ESG funds from HUD and make these funds available to eligible sub recipients, which can be either local government agencies or private nonprofit organizations.
- Policy/Advocacy Representative: Individual(s) who represent local government, county or state agency, AHCCCS, advocacy or policy-making group, member of the MAG Regional Domestic Violence Council, or other local policy/advocacy group recommended by the Continuum of Care.
- CoC-Funded Provider Representative: An agency that operates a Continuum of Care Program funded homeless assistance program.
- Funder: A local agency that funds homeless services and housing programs in Maricopa County. This could include a philanthropic funder, a municipality, United Way, or other funder recommended by the Continuum of Care.
- Community Seat: Individual(s) who represent the public housing authorities, businesses, faith-based organizations, jails, hospitals, universities, or other community seat as recommended by the Continuum of Care.

The three CoC funded provider seats on the Board will represent one or more of the following homeless subpopulations:

a) Single individuals
b) Families with children
c) Veterans
d) Persons who are chronically homeless
e) Persons with HIV/AIDS
f) Unaccompanied youth
g) Persons with behavioral health issues
h) Persons who are victims of domestic violence

Membership Selection

The second element is recruitment and selection of the members for each CoC Board seat. The process to select the CoC Board membership will be transparent, inclusive, and democratic in nature. The CoC Board member selection process will include consideration of geographic balance, representation of homeless subpopulations, and knowledge of the issues pertaining to the Continuum of Care and/or persons experiencing homelessness in the region.

When a vacancy occurs, a Membership Workgroup may be formed to recommend new members **if** the Board decides to recruit new members. If the current membership consists of seven or more members, the Board may decide not to add members. If the Board decides to add members, the Membership Workgroup may include members of the Board, members of the Committee, members of PSDQ, members of the CEOWG, and members of the community with a total of seven members. To solicit new Board members, an invitation will be extended by the collaborative applicant to the CoC Committee and stakeholders requesting potential members to submit ~~letters of interest~~ a resume and complete a brief application. The collaborative applicant will prepare a list of people who submitted ~~letters of interest~~ applications with the category(ies) they represent to the Membership Workgroup. The Membership Workgroup will review the list, resumes and ~~letters~~ applications and make recommendations to the CoC Board for membership. The CoC Board will review recommendations~~, as well as the list and letters,~~ and vote to fill vacancies on the Board. Members cannot vote for themselves. The CoC Board will base the decision on ensuring diverse representation on the Board in compliance with the HEARTH Act Interim Rule and local priorities.

Once the first Board has been established, staggered term limits will apply with 33 percent of the board rotating off every year. The initial rotation will begin with one third of the membership serving a two year term, one third serving a three year term, and one third serving a four year term with all members serving staggered three year terms thereafter. Members may choose to extend their terms for one additional three-year term, but must rotate off the Board for at least one year following the second term before seeking to rejoin the Board. In cases of vacancies in the middle of a term, the new member filling the vacant positon will be elected to a new three-year term and will not be held to the remaining term of the vacant position.

Exceptions may be made to the term limits with approval from the Board if no other members can be found to represent a certain category.

Ongoing Analysis of Membership