HOMELESS MANAGEMENT INFORMATION SYSTEM
YOUNGSTOWN/MAHONING COUNTY, OHIO

Policies and Procedures Manual
V 4.0

Project of the Mahoning County Homeless Continuum of Care
Administered by Catholic Charities Regional Agency

HOMELESS MANAGEMENT INFORMATION SYSTEM

Policies and Procedures Manual

HMIS Lead Agency/ Mahoning County Homeless Continuum of Care
Catholic Charities Regional Agency
319 W. Rayen Avenue
Youngstown OH 44502
(P) 330-744-3320 (F) 330-744-3677

TABLE OF CONTENTS

Section #	Section Name	Page #(s)
Section 1	**Participation Requirements and Contracts**	
1.1	HUD HMIS Agency Participation Requirement	4
1.2	HMIS Advisory Committee	4-5
1.3	HMIS Partner Agency Participation	5-6
1.4	Role of Security Officer and Execution of Administrator Agreement	6
1.5	Role of End User(s) and Execution of User Agreement(s)	6
Section 2	**CCRA Scope of Services**	
2.1	Project Management	7
2.2	Hardware Requirements, Ownership and Maintenance	7
2.3	Internet Connectivity	7
2.4	CCRA Contract with Mediware System	8
2.5	Communication	8
2.6	Implementation and Refresher Software Training Program	8
2.7	User Group Meetings	8
2.8	Technical Assistance Delivery Plan	8-9
Section 3	**Privacy Standards**	
3.1	Compliance with Privacy Rules	9
3.2	Privacy Rule Exemption, HIPAA Covered Entities	9
3.3	Allowable Uses and Disclosures	10
3.4	Data Collection and Notification	10
3.5	Client Consent: Oral or Written	10-11
3.6	Privacy Notice: Purpose Specification and Use Limitation	11
3.7	Privacy Notice: Openness	11
3.8	Privacy Notice: Access and Correction	11-12
3.9	Privacy Notice: Accountability	12
3.10	CCRA Privacy Monitoring	12-13
Section 4	**System Security and Hard Copy Security Standards**	
4.1	Security Rule Exemption, HIPAA Covered Entities	13
4.2	Data Access Location	13
4.3	Physical Access to Systems with Access to HMIS Data	13-14
4.4	System User Authentication: User ID and Password	14
4.5	Virus Protection	14
4.6	Firewalls	14
4.7	System Monitoring	14-15
4.8	Disaster Protection and Recovery	15
4.9	Disposal	15
4.10	Extracted Data	15
4.11	Hard Copy Security	15-16
4.12	CCRA System Monitoring	16
Section 5	**Application Security Standards**	
5.1	User Access	16
5.2	User Access Levels	16
5.3	Application User Authentication	16-17
5.4	Application User Authentication: Multiple Access	17

5.5	Electronic Data Transmission	17
5.6	Electronic Data Storage	17
5.7	Application Monitoring	18
Section 6	**Data Collection, Entry, and Quality**	
6.1	System Availability	18
6.2	Appropriate Data Collection and Entry	18
6.3	Required Data Collection and Entry	18
6.4	Data Quality Plan	18
6.5	Data Quality Standard: Accuracy	19
6.6	Data Quality Standard: Timeliness	19
6.7	Data Quality Monitoring	19
Section 7	**Data Usage and Release**	
7.1	Partner Agency	19
7.2	CCRA/System Administration	19
7.3	CCRA/Public Release	19
Section 8	**Data Sharing**	
8.1	Data Sharing Availability	19-20
8.2	Data Sharing Authorization	20
8.3	Release of Client Information	20
8.4	Data Quality	20
8.5	Monitoring	20
	Attachment A - MCHCOC HMIS Partner Agencies	21-22
	Attachment B - Partner Agency Participation Agreement	23-29
	Attachment C - Security Officer Agreement	30
	Attachment D - End User Agreement: Responsibility Statement and Code of Ethics	31-33
	Attachment E - Authorization for the Release of Information	34
	Attachment F - Privacy Policy	35-37
	Attachment G - Consumer Notice	38
	Appendix A – Data Elements	39-40

Definitions

HMIS – Homeless Management Information System is a data collection tool that maintains information regarding the demographics, characteristics and service needs of homeless, and those at-risk of homelessness, in order to provide and coordinate programs and services more effectively throughout the Mahoning County.

HMIS System Administrator (SA) – The person in charge of the project management of HMIS; including training End Users, vendor contract management, local software configuration, and reporting on the HMIS to the Continuum of Care and participating agencies.

Continuum of Care (CoC) – the participating agencies and stakeholders that provide services to homeless and near homeless individuals and families. This group of stakeholders also includes homeless and formerly homeless individuals, government officials, businesses and any interested parties seeking to support the service needs of homeless and those at-risk of homelessness.

ServicePoint –The HMIS web-based software that is currently used by the CoC and is licensed from Mediware Systems, LLC.

Participating Agency (PA) – Any agency within the CoC that has an agency agreement and a license to use HMIS.

Partner Agency Participation Agreement – A signed agreement between the HMIS Administering Agency, Catholic Charities Regional Agency (CCRA), and the PA entering data into ServicePoint.

Client – Any person who has Personal Protected Information entered into HMIS.

Personal Protected Information (PPI) – is any information maintained about a client that allows identification of an individual directly or indirectly; can be manipulated by a reasonably foreseeable method to identify a specific individual, or can be linked with other available information to identify a specific client.

Security Officer (SO) – the End User, who is trained by the System Administrator, and responsible for security compliance at the Participating Partner Agency.

Security Officer Agreement – A signed agreement between the HMIS Administering Agency (CCRA) and the Security Officer entering data into ServicePoint.

End User –A person from a participating agency that has been fully trained by the HMIS Administrator to enter data into ServicePoint. This person is charged with the responsibility to ensure that all data is accounted for and accurate. Every End User must sign a User Participation Agreement.

End User Agreement – A signed agreement between the HMIS Administering Agency (CCRA) and the End User entering data into ServicePoint.

Consumer Notice – The HUD mandated notice that must be posted at client intake that notifies the client of their rights related to HMIS data collection and use.

Privacy Notice- The HUD mandated privacy policy that every Participating Agency must have as part of their organization's policies related to client privacy.

SECTION 1: PARTICIPATION REQUIREMENTS AND CONTRACTS

1.1 HUD HMIS Agency Participation Requirement

1.5.1. Participation Requirements for Providers Receiving HUD McKinney-Vento Act Funding, (Docket No. FR 4848-N-02), 2004 Federal Register, Vol. 69, **Pages 45901-45902**

All program recipients of the HUD McKinney-Vento Act, as amended by S. 896 The Homeless Emergency Assistance and Rapid Transition to Housing (HEARTH) Act of 2009 funds are required to participate in the HMIS. The HUD McKinney Vento Act programs include **ESG, SHP, S+C, and Section 8 Moderate Rehabilitation for SRO** and HOPWA. In FY 2003 funding notices for SHP, S+C, and Section 8 Moderate Rehabilitation for SRO programs, HUD announced that providing data to an HMIS is a condition of funding for grantees. As part of the Federal Strategic Plan to End Homelessness, in 2012 the following Federal Agencies required that funding for homeless and homeless prevention activities from the following federal programs are mandated to participate in HMIS: Federal Department of Veterans Administration, Federal Department of Health and Human Services, Federal Department of Veterans Administration programs that are required to participate in HMIS include **Grant Per-Diem Funds, HealthCare for Homeless Veterans Community Contract Beds, and Supportive Services for Veteran Families**. The Federal Department of Health and Human Services programs that are required to participate in HMIS include **Projects for Assistance in Transition from Homelessness (PATH), Runaway Homeless and Youth programs including (Basic Center Program, Transitional Living Program, Street Outreach Program).** Locally, agencies funded by HUD through the Mahoning County Homeless Continuum of Care *(herein referred to as the CoC)* and agencies receiving Emergency Solutions Grant funding to provide homeless programs in the City of Youngstown and/or Mahoning County are required to participate in the HMIS. While the CoC cannot require non-funded providers to participate in the HMIS, they will work closely with them to articulate the benefits of the HMIS and to strongly encourage their participation in order to achieve a comprehensive and accurate understanding of homelessness in Mahoning County. See Attachment A, Mahoning County Homeless Continuum of Care HMIS Partner Agencies, for a complete list of participating agencies/programs.

1.2 HMIS Advisory Committee

The HMIS Advisory Committee guides the planning and implementation of the HMIS project by providing policy, technical and organizational assistance. Ongoing input is sought from service providers and community stakeholders.

The committee reports to the Executive Board and the full Continuum and may propose policies and other actions to the Continuum for its consideration. The HMIS Committee serves as an advisor to the HMIS lead agency, Catholic Charities Regional Agency (CCRA) and to the contracted HMIS Administrator, COHHIO (Coalition on Housing and Homelessness in Ohio). The final decision-making authority is CCRA provided they are responsible for the Supportive Housing Program funding from the U.S. Department of Housing and Urban Development (HUD).

Committee Membership
The HMIS Advisory Committee will be established according to the following guidelines:

- Target membership will be no less than 6 persons;
- The HMIS Advisory Committee Chair and HMIS Lead will convene and facilitate the advisory committee.
- There will be a proactive effort to have representation from shelters/transitional housing for families and individuals, other homeless services organizations and government agencies that fund homeless assistance services.
- HMIS Advisory Committee members must attend a minimum 75% of meetings. If the member cannot attend, he or she must send a replacement. There will be a concerted effort to find replacement representatives when participation has been inactive or inconsistent or below 75%.

The committee will meet at a frequency as specified below:

- Monthly or as needed

Responsibilities of the HMIS Advisory Committee
The members of the HMIS Advisory Committee are *voluntary, non-paid positions***,** who:

- Plan, facilitate, and evaluate HMIS implementation
- Develop and review policies related to HMIS
- Assist in developing common system documents or reports
- Set minimal data collection requirements
- Participate in the Point-In-Time
- Conduct Gaps Analysis and Housing Inventory
- Define criteria, standards and parameters for release of aggregate data
- Encourage Continuum-wide provider participation in HMIS
- Gather and coordinate resources and /or incentives to assist providers with participation
- Assist in identifying public and private funds to continue HMIS operation
- Report to funders and the community on homeless using HMIS data
- Respond to community questions about homeless populations
- Serve as a review and appeal for actions that CCRA may take or request to take involving a member agency that is non-compliant with the *Partner Agency Participation Agreement* (Attachment B).

1.3 HMIS Partner Agency Participation

Only agencies that have agreed to the terms set out in the *Partner Agency Participation Agreement* are granted access to the HMIS. This agreement provides Partner Agencies with clear expectations for participation and includes terms and duration of access, an acknowledgement and receipt of the Policies and Procedures Manual, and an agreement to abide by all provisions contained therein. Through execution of this agreement, Partner Agencies commit to collaborate with CCRA, COHHIO and the CoC for effective use of the system. This agreement must be signed by the HMIS Lead Agency and Agency Executive Director.

All End Users must attend the required training before access to HMIS is granted. End Users must log into HMIS no more than one month after this agreement is signed. Continued use of HMIS is required to keep the license assigned by the SA. This usage will be monitored through audit reports run by the SA. If an End User does not log into ServicePoint at least quarterly, the SA may revoke access and reassign the license to another agency or end user. All End Users must attend mandatory ongoing trainings or their license will become inactive until the training is completed.

1.4 Role of Agency Security Officer and Execution of Agency Security Officer Agreement

Each Partner Agency must designate a HMIS Security Officer (herein referred to as SO), approved and trained by the SA. The SO is the primary HMIS contact at the Partner Agency and the individual who provides a single point of communication between End Users and CCRA's HMIS System Administrator (herein referred to as SA). Designating a primary HMIS contact at each Partner Agency increases the effectiveness of communication between the SA and Partner Agencies and both between and within agencies. SOs are responsible for the security, confidentiality, and quality of their Agency's Client data within the HMIS. Security training is mandatory for every security officer annually, and will be provided by the HMIS staff.

SO responsibilities include:

1. All activity associated with the Partner Agency including oversight of agency staff who have access to ServicePoint.
2. The designated employee must execute a *Security Officer Agreement* (Attachment C). This agreement must be signed by the Agency Executive Director and HMIS Security Officer and submitted to CCRA.
3. Ensure that access to ServicePoint is granted to staff only after they have received training and executed a *User Agreement Responsibility Statement and Code of Ethics* (Attachment D).
4. Allow access to ServicePoint based upon need. Need exists only for those staff who work directly with (or supervise staff who work directly with) Clients or have data entry responsibilities.
5. Enforce business controls and practices to ensure organizational adherence to the HMIS policies and procedures, including the following:
    - monitor compliance with standards of Client confidentiality and ethical data collection, entry, and retrieval;
    - ensure completeness and accuracy of Client-level data entered into the HMIS;
    - monitor and take appropriate action if misuse of ServicePoint occurs including failure to perform duties as outlined in End User Agreements.
6. Provide support for the generation of agency reports, including the HUD CoC APR.
7. Ensure the stability of the agency connection to the Internet and ServicePoint, either directly or in communication with other technical professionals.
8. It is strongly recommended that the SO represent their Partner Agency on the HMIS Advisory Committee.

1.5 Role of End User and Execution of User Agreement

Each Partner Agency must designate an End User(s). End Users are responsible for entering and managing Client data within the HMIS. Each End User must execute a *User Agreement: Responsibility Statement and Code of Ethics*. The *User Agreement* provides documentation that the End User received training, will abide by the HMIS Policies and Procedures Manual, will appropriately maintain the confidentiality of Client data, and will only collect, enter, and retrieve data in the HMIS relevant to the delivery of services to the homeless population in Youngstown and Mahoning County. This agreement acknowledges receipt of a copy of the Agency's *Privacy Notice* and requires End Users to pledge to comply with it. This agreement must be signed by the Partner Agency Executive Director and End User and submitted to CCRA. The SO is also considered an End User and must also sign the *User Agreement*.

SECTION 2: CCRA SCOPE OF SERVICES

2.1 Project Management

Catholic Charities Regional Agency (herein referred to as CCRA), in accordance with a Memorandum of Understanding between the Mahoning County Homeless Continuum of Care, and COHHIO, in accordance with agreement with CCRA, is responsible for project coordination and management, system administration, training and technical support, and data analysis and reporting.

Responsibilities:

1. Provide on-going outreach to agency and community leadership to cultivate and maintain support and understanding of HMIS issues.
2. Oversight of all contractual agreements with Partner Agencies.
3. Manage Partner Agency and End User system access based on execution of applicable agreements, training, and adherence to approved policies and procedures.
4. Facilitate HMIS policies and procedures development, focusing on privacy, security and data standards and data usage and release.
5. Supervise contractual relationship with ServicePoint.
6. Set-up and management of ServicePoint End User accounts, access levels, and passwords, in conjunction with COHHIO.
7. Facilitate software (ServicePoint) training and technical support with COHHIO.
8. Provide End User support for ServicePoint, including coordination of End User meetings to address data entry problems and troubleshooting, in conjunction with COHHIO.
9. Maintain overall quality assurance program including monitoring of integrity of data collected and data collection practices.
10. Audit usage and access of the HMIS database.
11. Generate program, agency, and CoC level data reports.

2.2 Internet Connectivity

(1) Connection to the Internet is the sole responsibility of Partner Agencies and is a requirement to participate in the HMIS. Any computer that connects to the HMIS must meet ServicePoint Internet connectivity specifications listed below. Partner Agencies must also provide internal technical support for the Internet connection according to their own organizational needs. Although there is no unusual software required to connect to the HMIS, the speed and quality of the Internet connection has a profound effect on the ease of data entry and report extraction.

2.3 CCRA Contract with Mediware Systems

The following software protocols are integrated into the project and are paid for by the current HUD grant for only current Partner Agencies: (1) Server Software License, (2) Thirty-one End User Licenses, (3) Annual Support, (4) Training Website and Annual Support, (5) Implementation Training, (6) Disaster and Recovery Protection, (7) SSL Certificate, and (8) AIRS Taxonomy License.

End User Licenses. Participating Partner Agencies received two ServicePoint End User licenses. New Partner Agency may obtain End User licenses at no additional cost, depending on funding available. In addition to licensing fees, new Partner Agencies may have to pay the hosting and annual support fees associated with User licenses. Mediware Systems, not CCRA, determines fees for User licenses, annual support, and server/hosting, therefore these fees are subject to change. The Partner Agency would provide a check to CCRA to cover the cost of the licenses

and associated fees. The SA purchases licenses online through the ServicePoint. Mediware Systems then invoices CCRA. The SA notifies the Partner Agency when the additional licenses are available.

2.4 Communication

CCRA, as HMIS Lead, and COHHIO, as the SA or HMIS administrator, communicates with Partner Agencies in a relevant and timely manner. The SA posts system-wide information via ServicePoint's System Newsflash. General communication from the SA is directed to SO and specific communication will be addressed to the person(s) involved. The SA is available via phone and email. Partner Agencies are responsible for communicating needs and questions regarding the HMIS directly to the SA. The SA responds to Partner Agency needs within 2 business days of the first contact.

2.5 Implementation and Refresher Software Training Program

COHHIO conducts the software implementation training program. The training program is a requirement for HMIS participation and covers agency administration, basic data entry, canned reports (HUD CoC APR), and data quality. COHHIO provides refresher training as needed and training following a system upgrade/new version releases. Training for new End Users, refresher training and special topic trainings are scheduled upon Agency request. All End Users must attend and complete mandatory trainings or their licenses status will become inactive until that training is completed.

2.6 Technical Assistance Delivery Plan

Standard Technical Assistance. COHHIO provides Partner Agencies with a help desk to access and use the HMIS. The help desk system provides End Users with a central resource to call or email questions and resolve software issues. Basic End Users support and technical assistance includes general troubleshooting and assistance with standard report generation. Send help desk requests to hmis@cohhio.org.

Web-based Technical Assistance. There will be occasions when an SA will request to use GoToMeeting or a similar program to view what the user is doing or seeing, and/or take control of the user's keyboard and mouse to demonstrate how to correct data. In every case, the user will be notified prior to moving to this type of assistance.

Onsite Technical Assistance. The SA conducts site visits as a part of the overall data quality plan and in response to Partner Agency requests. The SA will also conduct site visits if a Partner Agency has significant data quality issues.

SECTION 3: PRIVACY STANDARDS

A majority of HMIS Privacy Standards in Section 3 are required by the Department of Housing and Urban Development's (HUD), pursuant to the "Homeless Management Information Systems (HMIS) Data and Technical Standards Notice" (Docket No. FR 4848-N-02). The Privacy Standards describe standards for the privacy of personal information collected and stored in a HMIS. The standards seek to protect the confidentiality of personal information while allowing for reasonable, responsible, and limited uses and disclosures of data. These privacy standards are based on principles of fair information practices recognized by the information privacy and technology communities. The Privacy Standards apply to all Partner Agencies or any Agency that records, uses, or processes PPI on homeless clients for an HMIS. All PPI maintained by a Partner Agency is subject to these standards. Partner Agencies must also comply with federal, state and local laws that require additional confidentiality protections. * Privacy Standards

mandated by HUD will be indicated as so by the number and name of the standard and page number.

3.1 Compliance with Privacy Rules

Partner Agency privacy practices shall comply with all applicable laws governing HMIS client privacy/confidentiality. Applicable standards include, but are not limited to the following:

1. Department of Housing and Urban Development's (HUD) "Homeless Management Information Systems (HMIS) Data and Technical Standards Notice" (Docket No. FR 4848-N-02).
2. Federal, state and local laws that require additional confidentiality protections.
3. Health Insurance Portability and Accountability Act of 1996, 45 CFR Parts 160 & 164.
4. Confidentiality of Alcohol and Drug Abuse Patient Records, 42 CFR Part 2.
5. All laws, statutes, administration, and rules that are specific to the services provided (for example, laws pertaining to mental health, substance abuse, and domestic violence).
6. Mahoning County HMIS Policies and Procedures and associated agreements (*Partner Agency Participation Agreement, User Agreement, and Security Officer Agreement).*

3.2 Privacy Rule Exemption, HIPAA Covered Entities

4.1.2 Applying the HMIS Privacy and Security Standards, PAGE 45928

Any Partner Agency covered under HIPAA is not required to comply with HMIS Privacy Standards (Docket No. FR 4848-N-02) if the Partner Agency determines that a substantial portion of its PPI about homeless clients or homeless individuals is protected health information as defined in the HIPAA rules. It is possible that part of a Partner Agency's operations may be covered by the HMIS standards while another part is covered by the HIPAA standards. A Partner Agency that, because of organizational structure, legal requirement, or other reason, maintains personal information about a homeless client that does not fall under the privacy and security standards in this section (*e.g.*, the information is subject to the HIPAA health privacy rule) must describe that information in its privacy notice and explain the reason the information is not covered. The purpose of the disclosure requirement is to avoid giving the impression that all personal information will be protected under the HMIS standards if other standards or if no standards apply.

3.3 Allowable Uses and Disclosures

4.1.3 Allowable Uses and Disclosures of Protected Personal Information (PPI), PAGES 45928-45929

PPI (protected personal information, that is, information which can be used to identify a client) can be used only for the following purposes:

(1) To provide or coordinate services to an individual.

(2) For functions related to payment or reimbursement for services.

(3) To carry out administrative functions, including but not limited to legal, audit, personnel, oversight and management functions.

(4) For creating de-identified PPI for unduplicated counting.

(5) Where the disclosure is required by law.

(6) To prevent or lessen a serious and imminent threat to the health or safety of an individual or the public.

(7) To report abuse, neglect, or domestic violence as required or allowed by law.

(8) Contractual research where privacy conditions are met (including a written agreement).

(9) For law enforcement purposes in response to a properly authorized request for information from a properly authorized source.

(10) To report criminal activity on agency premises.

HMIS Privacy Standards (Docket No. FR 4848-N-02) list items 1-4 as allowable uses and disclosures for disclosing PPI but makes provisions for additional uses and disclosures, items 5-10, to meet Partner Agency obligations. Partner Agencies should include all standard uses and disclosures in their Privacy Notice unless there is specific justification to do otherwise. Partner Agencies may decline even to reserve the option to make a use or disclosure from standard list by not including it in its Privacy Notice. It would clearly be appropriate to do so, for example, if a state law prohibited a particular use or disclosure.

3.4 Data Collection and Notification

4.2.1 Collection Limitation, Baseline Requirement, PAGE 45929

Partner Agencies may collect PPI only when appropriate to the purposes for which the information is obtained or when required by law. Partner Agencies must collect PPI by lawful and fair means, and, where appropriate, with the knowledge or consent of the individual.

(1) Partner Agencies must collect PPI only for the purposes listed in 5.3.

(2) Partner Agencies must make clients aware that personal information is being collected, recorded and shared.

(3) Partner Agencies must post the *HMIS Consumer Notice* provided by CCRA at each intake desk or comparable location that generally explains the reason for data collection. If an Agency places the *HMIS Consumer Notice* in a comparable location, it must be a prominent location where it is reasonable to expect Clients to be able to read the Notice.

(4) Partner Agency staff must thoroughly explain the *HMIS Consumer Notice* to each Client.

3.5 Client Consent: Written Release of Information

4.2.1. Collection Limitation, Additional Privacy Protections, PAGE 45929

Partner Agencies must obtain written consent for the collection of all data from Clients. Written Consent must be obtained using the universal CoC approved *Mahoning County HMIS Authorization for Release of Information* form (Attachment E). Partner Agencies must obtain a separate consent form for each member of the household receiving services.

Partner Agencies must place all *Mahoning County HMIS Authorization for Release of Information (ROI)* forms in a file to be located at Agency's business address and that such forms will be made available to the SA for periodic audits. Partner Agencies must retain these forms for a period of 7 years after program exit, at which time the forms can be discarded in a manner that ensures Client confidentiality is not compromised.

3.6 Privacy Notice, Purpose Specification and Use Limitation

4.2.2. Purpose Specification and Use Limitation, Baseline Requirement, PAGE 45930

The purposes for collecting PPI, as well as its uses and disclosures are specified and limited.

(1) Partner Agencies must publish the CoC Universal HMIS *Privacy Notice* (Attachment F). Partner Agencies must adopt this HMIS *Privacy Notice* as part of their organization's Policies and Procedures. This is HUD's Baseline Model Privacy Notice for Homeless Organizations.

(2) Partner Agencies must specify in the *Privacy Notice* the purposes for collecting PPI and describe all uses and disclosures.

(3) Partner Agencies may use or disclose PPI only if the use or disclosure is allowed by HMIS Privacy Standards (Docket No. FR 4848-N-02) and described in the HMIS *Privacy Notice*.

(4) Partner Agencies must have signed written consent from the Universal Release of Information Form for all uses and disclosures specified in the HMIS *Privacy Notice* and for uses and disclosures determined by the Partner Agency to be compatible with those specified in their *Privacy Notice*.

(5) Partner Agencies must obtain Client consent for uses and disclosures not specified in their *Privacy Notice*.

3.7 Privacy Notice, Openness

4.2.4. Openness, Baseline Requirement, PAGE 45930

(1) Partner Agencies must publish a *Privacy Notice* describing its policies for the processing of PPI and must provide a copy of its *Privacy Notice* to Clients upon request.

(2) Partner Agencies must post a sign, the *HMIS Consumer Notice* (Attachment G), stating the availability of the HMIS *Privacy Notice* to any Client who requests a copy.

(3) Partner Agencies that maintain a public web page, may post the current version of the HMIS *Privacy Notice* on their web page. The street address may be omitted.

3.8 Privacy Notice, Access and Correction

4.2.5. Access and Correction, Baseline Requirement, PAGE 45930

(1) In general, Partner Agencies must allow Clients to inspect and to have a copy of any PPI about him or her.

(2) Partner Agencies must also offer to explain any information that the Client may not understand.

(3) Partner Agencies must consider any request by Clients for correction of inaccurate or incomplete PPI pertaining to the individual. Partner Agencies are not required to remove any information but may, in the alternative, mark information as inaccurate or incomplete and may supplement it with additional information.

(4) In their *Privacy Notice*, Partner Agencies may reserve the right to deny an individual inspection or copying of the individual's PPI for the following reasons:

(a) Information compiled in reasonable anticipation of litigation or comparable proceedings.

(b) Information about another individual (other than a health care or homeless provider).

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

(d) Information, the disclosure of which would be reasonably likely to endanger the life or physical safety of any individual.

(5) Partner Agencies can reject repeated or harassing requests for access or correction. A Partner Agency that denies a Client's request for access or correction must explain the reason for the denial to the Client and must include documentation of the request and the reason for the denial as part of the protected personal information about the Client.

3.9 Privacy Notice: Accountability

4.2.6. Accountability, Baseline Requirement, PAGE 45931

(1) Partner Agencies are responsible for answering questions and addressing complaints from their own Clients regarding the HMIS. Partner Agencies must describe grievance procedures in their *Privacy Notice*.

(2) Partner Agencies must establish a grievance procedure for accepting and considering questions or complaints about its privacy and security practices. Partner Agencies must add the following statement to their grievance procedure: "For Mahoning County HMIS-related grievances, a copy of the grievance and (Agency's name) response to that grievance will be forwarded to the HMIS System Administrator." Partner Agencies are obligated to report all HMIS-related grievances to the SA, who documents and summarizes all grievances and resolutions. This information is made available to the HMIS Advisory Committee to determine the need for further action, if any. These actions might include further investigation of incidents, clarification or review of policies, or sanctioning of End Users and agencies if End Users or agencies are found to have violated standards set forth in HMIS Agency Agreements or the Policies and Procedures Manual.

(3) Partner Agencies must require each member of its staff (including employees, volunteers, affiliates, contractors and associates) to sign (annually or otherwise) a confidentiality agreement that acknowledges receipt of a copy of the *Privacy Notice* and that pledges to comply with the *Privacy Notice*.

3.10 CCRA Privacy Monitoring

Partner Agencies must permit the SA to monitor and periodically audit its handling of confidential Client data in connection to the HMIS, including but not limited to, its confidentiality procedures. The SA performs privacy audits to ensure Agency is in compliance with the Department of Housing and Urban Development's (HUD) "Homeless Management Information Systems (HMIS) Data and Technical Standards Notice" (Docket No. FR 4848-N-02).

Findings for monitoring noncompliance

Violation: PPI (Protected Personal Information) can be used only for the stated purposed above. Any violation may result in the following actions:

First offense – if client information is breached in a detrimental manner, the violator will be prohibited from further HMIS participation and all rights and access to HMIS will be revoked. If client information is not breached in a detrimental manner, a period of suspension from HMIS may be considered. Further action may be taken by the HMIS Advisory Committee and SA.

Second offense – if client information is breached a second time the violator will be prohibited from further HMIS participation and all rights and access to HMIS will be revoked.

SECTION 4: SYSTEM SECURITY AND HARD COPY SECURITY STANDARDS

A majority of the Security Standards in Section 4 are required by the Department of Housing and Urban Development's (HUD) pursuant to the "Homeless Management Information Systems (HMIS) Data and Technical Standards Notice" (Docket No. FR 4848-N-02). HUD requires Partner Agencies to apply system security provisions to all the systems where personal protected information is stored, including, but not limited to, a Partner Agency's networks, desktops, laptops, mini-computers, mainframes, and servers. * Security Standards mandated by HUD will be indicated as so by the number and name of the standard and page number.

4.1 Security Rule Exemption, HIPAA Covered Entities

Applying the HMIS Privacy and Security Standards

Any Partner Agency covered under HIPAA is not required to comply with HMIS Security Standards (Docket No. FR 4848-N-02) if the Partner Agency determines that a substantial portion of its PPI about homeless clients or homeless individuals is protected health information as defined in the HIPAA rules. It is possible that part of a Partner Agency's operations may be covered by the HMIS standards while another part is covered by the HIPAA standards. A Partner Agency that, because of organizational structure, legal requirement, or other reason, maintains personal information about a homeless client that does not fall under the privacy and security standards in this section (*e.g.*, the information is subject to the HIPAA health privacy rule) must describe that information in its privacy notice and explain the reason the information is not covered. The purpose of the disclosure requirement is to avoid giving the impression that all personal information will be protected under the HMIS standards if other standards or if no standards apply.

4.2 Data Access Location

All End Users are prohibited from accessing the HMIS from any location other than the designated and approved HMIS workstations at the Partner Agency. Working at home or from a public location such as a library is strictly prohibited. SO must monitor End User compliance with this policy.

4.3 Physical Access to Systems with Access to HMIS Data

4.3.1. System Security, Physical Access to Systems with Access to HMIS Data, Additional Security Protection, PAGE 45932

Partner Agencies must limit physical access to HMIS systems (networks, severs, mainframes, desktops, laptops, and minicomputers) used to collect and store personal protected information (PPI) at all times. Partner Agencies must place computers used to connect to the HMIS in a private location unless deemed impossible. If a private location is deemed impossible, Partner Agencies must staff computers stationed in public areas at all times. When workstations are not in use and staff are not present, steps should be taken to ensure that 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 Partner Agencies. Mediware Systems employs auto-logout. When an End User's account is inactive for more than 30 minutes, ServicePoint automatically logs End Users out of the system. However, it is important to note that the last accessed page will remain visible on the End User's computer screen, therefore, End Users should always log out of the system prior to leaving their computer unattended for any amount of time. If the screen is left open to a Client record, there is a potential for a breach in Client confidentiality. If End Users will be gone for an extended period of time, End Users should log off of ServicePoint and shut down the computer.

4.4 System User Authentication: End User ID and Password

4.3.1. System Security, End User Authentication, Baseline Requirement, PAGE 45931

Partner Agencies must secure HMIS systems with, at a minimum, an End User authentication system consisting of an End User ID and password. End User authentication is the process of verifying that End Users are who they claim to be when logging into the HMIS workstation. Unique End User IDs and passwords are the basic building block of system security. SO, technical staff, or management set-up End User accounts and default passwords. End Users create their own passwords based on the requirements listed below. Passwords must be at least

eight characters long and meet reasonable industry standard requirements. These requirements include, but are not limited to:

(1) Using at least one number and one letter;
(2) Not using, or including, the End User ID, the HMIS name, or the HMIS vendor's name; and/or
(3) Not consisting entirely of any word found in the common dictionary or any of the above spelled backwards.

End Users are responsible for keeping their own passwords confidential. End User IDs and passwords cannot be stored or displayed in a publicly accessible location.

4.5 Virus Protection

4.3.1. System Security, Virus Protection, Baseline Requirement, PAGE 45931

Partner Agencies must protect Mahoning County HMIS systems (computers, networks, etc.) from viruses by using commercially available anti-virus software. Partner Agencies must install anti-virus software with automatic update or regularly update virus definitions from the software vendor. Virus protection reduces the threat of HMIS system attack and destruction of Client PPI.

4.6 Firewalls

4.3.1. System Security, Firewalls, Baseline Requirement, PAGE 45931

Partner Agencies must protect HMIS systems from malicious intrusion behind a secure firewall. A firewall is a hardware device or software application which blocks all incoming electronic traffic except traffic that is explicitly permitted. Each individual workstation does not need its own firewall, as long as there is a firewall between that workstation and any systems, including the Internet and other computer networks, located outside of the organization. For example, a workstation that accesses the Internet through a modem would need its own firewall. A workstation that accesses the Internet through a central server would not need a firewall as long as the server has a firewall.

4.7 System Monitoring

4.3.1. System Security, System Monitoring, Baseline Requirement, PAGE 45932

Partner Agencies must use appropriate methods to monitor security systems. In general, the purpose of auditing is to record certain types of actions to a log, so that a System Administrator can review logs and detect unauthorized activity. Specifically, monitoring can detect when, how, and who accessed, damaged, altered, or stole HMIS data. In addition to investigating security incidents, monitoring detects errors and viruses and hardware and software problems. Partner Agencies must maintain a User access log for all systems that have access to HMIS data, and check logs routinely.

4.8 Disaster Protection and Recovery

4.3.1. System Security, Disaster Protection and Recovery, Baseline Requirement

Mediware Systems provides basic disaster recovery which includes a daily back-up of the system, a remote fully configured host site with an emergency server, nightly data duplication to the emergency server, and 24/7 support. Mediware also employs appropriate physical protection controls (temperature control, fire suppression systems, and surge suppressors). Because Mediware Systems provides disaster protection and recovery, no other steps need to be taken by Partner Agencies.

4.9 Extracted Data

Partner Agencies must maintain the security of any Client PPI extracted from the HMIS and stored locally, including all data used in ServicePoint's custom reporting. The custom report-writer function of ServicePoint allows Client data to be downloaded to an encrypted file on local computers. Once that file is unencrypted by the User, PPI is left vulnerable on the local computer unless additional measures are taken. Such measures might include restricting access to the file by adding a password. Partner Agencies must not transmit any Client data outside of the private local area network unless it is properly protected. Partner Agencies assume full responsibility for the security and confidentiality of any and all data that is downloaded from the HMIS and on stored on Agency local computers.

4.10 Hard Copy Security

4.3.3. Hard Copy Security, Baseline Requirement, PAGE 45933

Partner Agencies must secure any paper or other hard copy containing personal protected information that is either generated by or for Mahoning County HMIS, including, but not limited to reports, data entry forms, and signed *Client Consent for HMIS Data Collection* forms. Partner Agencies must supervise at all times any paper or other hard copy generated by or for HMIS that contains PPI when the hard copy is in a public area. When staff are not present, the information must be secured in areas that are not publicly accessible. Written information specifically pertaining to End User access (*e.g.*, End User ID and password) must not be stored or displayed in any publicly accessible location.

4.11 CCRA System Monitoring

Partner Agencies must permit the SA to monitor and periodically audit its security practices in connection to the HMIS. The SA performs security audits to ensure each Agency is in compliance with the Department of Housing and Urban Development's (HUD) "Homeless Management Information Systems (HMIS) Data and Technical Standards Notice" (Docket No. FR 4848-N-02).

Any violations of the System Security and Hard Copy Security Standards may result in the following actions:
First Offense – written warning to include the corrective measures
Second Offense – suspension or removal of HMIS participation

SECTION 5: APPLICATION SECURITY STANDARDS

A majority of Security Standards in Section 5 are required by Department of Housing and Urban Development's (HUD), pursuant to the "Homeless Management Information Systems (HMIS) Data and Technical Standards Notice" (Docket No. FR 4848-N-02). HUD requires HMIS Partner Agencies to apply application security provisions to the software during data entry, and review or any other processing function. Application security, as defined by HUD, is how all HMIS data are secured by the HMIS application software. * Security Standards mandated by HUD will be indicated as so by the number and name of the standard and page number.

5.1 End User Access

Partner Agencies determine which employees are granted access to the HMIS. Eligibility is restricted to paid staff of Partner Agencies. If an agency wants to provide a license to a volunteer or unpaid staff, that request needs to be approved by the HMIS Lead. SOs can redistribute ServicePoint End User licenses to accommodate agency reorganization, provided the End User

has attended all required training and has the required signed agreements with CCRA in place. SOs must notify the SA immediately when an End User no longer requires access.

5.2 End User Access Levels

Access to the HMIS will be controlled based on End User needs. Need exists only for those designated personnel who work directly with (or supervise staff who work directly with) clients or have data entry responsibilities. All End Users will have an appropriate level of access to HMIS data - the level of access which allows efficient job performance without compromising the security of the HMIS or the integrity of Client data. A model of least-privilege is used; no End User is granted more than the least amount of privilege needed to perform his/her job. ServicePoint allows multiple levels of End User access to data contained in HMIS database. SOs must assign appropriate End User levels when adding new End Users. The SA offers procedural suggestions to avoid granting higher levels of access than are necessary for efficient job performance.

5.3 Application End User Authentication

Application Security, End User Authentication, Baseline Requirement

Partner Agencies must secure all electronic HMIS data with, at a minimum, an End User authentication system consisting of a User ID and password. End User authentication is the process of verifying that End Users are who they claim to be when logging into ServicePoint. Unique End User IDs and passwords are the basic building block of data security. Sharing of ServicePoint passwords is strictly prohibited and sanctions will be imposed on the End User and/or agency if End User account sharing occurs. ServicePoint passwords must be 8-16 characters long with a minimum of two numbers. HUD also requires passwords to meet the following reasonable industry standard requirements. These requirements include, but are not limited to:

(1) Using at least one number and one letter;

(2) Not using, or including, the End User ID, HMIS name, or HMIS vendor's name; and/or

(3) Not consisting entirely of any word found in the common dictionary or any of the above spelled backwards.

End Users are responsible for keeping their ServicePoint passwords confidential. End User ID's and passwords cannot be stored or displayed in a publicly accessible location.

5.4 Application End User Authentication: Multiple Access

Application Security, End User Authentication, Baseline Requirement

Partner Agencies must ensure that End Users are not able to log on to more than one workstation at a time, or able to log on to the network at more than one location at a time. Mediware Systems does not permit End Users to access ServicePoint from multiple computers concurrently. If an End User attempts to log in from another computer while they are currently logged in, an error will display and notification is sent to Mediware Systems' System Administrator. Because Mediware Systems does not permit multiple access, no other steps need to be taken by Partner Agencies.

5.5 Electronic Data Storage

Application Security, Electronic Data Storage, Baseline Requirement

Mediware Systems hosts the Mahoning County HMIS, and, therefore, all HMIS data are stored in this location. Mediware Systems employs Microsoft SQL 2000 server which already stores data in binary format. Because Mediware Systems already stores Mahoning County HMIS data in a binary format, no other steps need to be taken by Partner Agencies.

5.6 Application Monitoring

ServicePoint automatically tracks access to every client record by use, date, and time of access. The SA audits access to the HMIS and overall system usage. Any violations of the data sharing policies and procedures may result in the following actions:

First Offense –written warning to include the corrective measures
Second Offense –suspension or removal of HMIS participation

SECTION 6: DATA COLLECTION, ENTRY, AND QUALITY

6.1 System Availability

Mediware Systems provides a highly available database server. A highly available data server affords Partner Agencies the opportunity to plan data entry, management, and extraction according to their internal schedules. The SA informs Partner Agencies in advance of any planned interruption in service via the listserv and ServicePoint's System Newsflash. The SA logs all downtime for purposes of system evaluation. Logs are a part of the process of evaluating the overall performance of the HMIS.

6.2 Appropriate Data Collection and Entry

Partner Agencies must only collect and enter Client data relevant to the delivery of services to people experiencing homelessness in Mahoning County.

6.3 Required Data Collection and Entry

Partner Agencies will collect all required sets of data variables for each client as determined by HUD Data Standards (see Appendix A for Required Data Elements). Appendix A will contain a listing of data elements to be collected for each client contact in accordance with federal regulations. These data elements may change as HUD HMIS Data and Technical Standards are revised and updated.

6.4 Data Quality Plan

PPI collected by Partner Agencies must be relevant to the purpose for which it is to be used. To the extent necessary for those purposes, PPI should be accurate, complete and timely. Partner Agencies must meet data quality standards. The SA and HMIS Advisory Committee will define a data quality plan that includes specific data quality standards, mechanisms for monitoring data quality, sanctions for non-compliance with standards, and assigned responsibilities. This policy will be amended to incorporate the data quality plan once developed.

6.5 Data Quality Standard: Accuracy

Users are responsible for the accuracy of their own data entry. Accurate data entry is essential to ensuring the usefulness of the HMIS. The SA performs regular data integrity checks to test the integrity of the data contained in the HMIS. Any patterns of error will be reported to the SO. Users are required to correct data entry techniques and are monitored for compliance.

6.6 Data Quality Standard: Timeliness

Partner Agencies must enter all data collected and services provided into HMIS within seven business days.

6.7 Data Quality Monitoring

The SO is to run monthly data quality reports and make corrections on a monthly basis. Data clean up must be conducted and verified within one month. The SA will determine exact procedures for application monitoring. Any violations of the data quality policies and procedures may result in the following actions:

First Offense –written warning to include the corrective measures
Second Offense –possible suspension or removal of HMIS participation

SECTION 7: DATA USAGE AND RELEASE

7.1 Partner Agency

Partner Agencies have access to retrieve any individual and aggregate data entered by their own agency/programs. Partner Agencies can create and run their own reports using agency-wide data. Report customization allows Partner Agencies to track progress in meeting agency-level goals. Partner Agencies are also encouraged to use their own HMIS data for program monitoring and evaluation, funding needs, and public relations provided Client confidentiality is maintained. CCRA will not release Agency-specific data without explicit written permission of the Partner Agency.

7.2 CCRA/System Administration

The SA has access to retrieve all data in the HMIS. The SA reviews data to administer the HMIS, for troubleshooting purposes, and for data quality/integrity testing.

7.3 CCRA/Public

CCRA, in the name of the MCHCoC, issues periodic public reports about homelessness in Mahoning County. CCRA only uses de-identified, aggregate (not Agency-specific) HMIS data for homeless policy and planning decisions, in preparing for federal, state, or local applications for homelessness funding, to demonstrate the need for and effectiveness of programs, and to obtain a system-wide view of program utilization in Mahoning County. No individually identifiable Client data is reported. The content of the reports reflect a commitment to Client confidentiality and ethical data use. Public reports are not released until the CoC is comfortable with the reliability of the data. Partner Agencies may use published HMIS data.

SECTION 8: DATA SHARING

8.1 Data Sharing Availability

Participating agencies will share client information with other participating agencies in order to coordinate assistance, provide referrals and more effectively serve their clients. Data sharing is not a requirement of participating agencies or the clients they serve, but is highly recommended. The ServicePoint database is a completely open system, thereby having all client records and information entered automatically shared by all participating agencies and programs within the system upon immediate data entry. This includes all PPI data as well as program specific information and services provided. It is the Participating Agency's responsibility to ensure they are meeting the client confidentiality needs by having all clients, including adult guardians of children sign the Universal Release of Information form (Attachment E) for every single person (adult and child) entered into HMIS. Data collected and shared is only to be used for its intended

purpose as described in Section 3.3 of this document. Only authorized users may view or update client data.

8.2 Data Sharing Authorization and Agreement

The SA must authorize data sharing between agencies and configure ServicePoint to allow this capability. All agencies that want to share data must enter into a *Data Sharing Agreement* with those agencies that data will be shared with.

8.3 Release of Client Information

A Universal Release of Information (ROI, Attachment E) form must be developed and approved by the SA and used by all participating agencies. All clients must sign the ROI before data can be shared. The parent or legal guardian must provide consent for each minor in the household to share data. If a ROI is not provided by the client, their data cannot be shared. The ROI for data sharing in HMIS does not allow an agency to release information about a client from the database. The agency must still follow their own procedures for information sharing outside HMIS.

8.4 Data Quality

When a client record is set-up, the originating End User must verify client authorization and is responsible for ensuring that the ROI is on file for every client they enter into the system. The End User entering the information is also responsible for the data quality of that information. Therefore, if data should be cleaned up, they must make any changes and/or corrections as determined by the SA.

8.5 Monitoring

Monitoring and enforcement of these policies will be conducted by the HMIS System Administrator. Any violations of the data sharing policies and procedures may result in the following actions:

First Offense –written warning to include the corrective measures
Second Offense –suspension or removal of HMIS participation

Mahoning County CoC HMIS Partner Agencies

HMIS Partner Agency	Homeless Program
Beatitude House	CH - Permanent Supportive Housing Program
Beatitude House	Permanent Supportive Housing Program
Catholic Charities Regional Agency	HCRP ODSA HP
Catholic Charities Regional Agency	HCRP ODSA RRH
Catholic Charities Regional Agency	ESG City HP
Catholic Charities Regional Agency	ESG City RRH
Compass Family and Community Service	Daybreak
Compass Family and Community Service	Sojourner House
Help Network NEO	Projects for Assistance in Transition from Homelessness (PATH)
Help Network NEO	PATH Trumbull
Help Network NEO	Shelter Plus Care
Help Network NEO	Coordinated Entry
Mahoning Valley Dispute Resolutions Services	ESG HP
Meridian Healthcare	Homeless Solutions SRO
Meridian Healthcare	Homeless Solutions SRO II
Meridian Healthcare	Homestead House
Meridian Healthcare	Phoenix Court
Meridian Healthcare	Project Safe
Meridian Healthcare	Samaritan House PRA
Rescue Mission of the Mahoning Valley	Mahoning Valley Family Services Division
Rescue Mission of the Mahoning Valley	Mahoning Valley Men's Division
Ursuline Center	Merici Housing PSH
Ursuline Center	Merici Living PSH
Ursuline Center	Merici Shelter (ES)
YWCA Mahoning Valley	Barbara M. Wick Transitional Home
YWCA Mahoning Valley	Permanent Housing for Disabled Families
YWCA Mahoning Valley	Scattered-sites Housing for Families with Disabilities, II

Homeless Program Type Total	Code Color/Homeless Program Type
13	Permanent Supportive Housing
1	Transitional Housing
5	Emergency Shelter
2	Street Outreach
3	Homeless Prevention
2	Rapid Re-Housing
1	Coordinated Entry
27	**TOTAL**

Mahoning County HMIS

PARTNER AGENCY PARTICIPATION AGREEMENT

The Mahoning County Homeless Management Information System, herein referred to as HMIS, is a software solution that maintains information regarding the demographics, characteristics and service needs of Participating Agency Clients in order to provide and coordinate programs and services more effectively.

(Agency Name)_____, has elected to participate in the Mahoning County HMIS, herein referred to as the HMIS. Participating agencies may elect to share client data. However it is not a requirement for HMIS participation or the clients they serve.

By checking the appropriate statement below, (Agency Name)_____verifies that it will comply with the following: **(check ONE statement below)**

(1)_____ will share client information with HMIS Participating Agencies in order to coordinate assistance, provide referrals and more effectively serve their clients:

(2)_____ will NOT share client information with HMIS Participating Agencies.

The signature of the Executive Director of the HMIS Partner Agency indicates agreement with the terms set forth before a HMIS account can be established for Agency, or further participation in HMIS can occur upon having an open system.

Catholic Charities Regional Agency, herein referred to as CCRA, is the primary coordinating institution and system administrator. In this Agreement, “Agency” is the Agency named in this agreement, “Partner Agency” is any Agency participating in the HMIS, and "Client" is a consumer of services.

I. Catholic Charities Regional Agency Scope of Services

(1) CCRA shall be responsible for project management of the HMIS. CCRA shall manage HMIS project operations, including, but not limited to: maintaining policies and procedures, managing Partner Agency contracts, participation and contract compliance, software provider relations, system administration and information security, training, technical support, data quality, and data analysis and reporting. CCRA shall manage the HMIS community including, but not limited to: communicating with stakeholders, working with the HMIS Advisory Committee, and working with HMIS user groups and working groups.

(2) CCRA views the HMIS as a "work in progress". CCRA shall work with Partner Agencies to ensure that the HMIS is responsive to changing and/or new needs as identified by Agencies and their End Users. This effort shall include enhancing HMIS functionality and capability.

(3) CCRA shall be responsible for relevant and timely communication with Agency regarding the HMIS. Agency shall be responsible for communicating needs and questions regarding the HMIS directly to CCRA.

(4) CCRA shall be the single point of contact with Mediware Systems and supervise the contractual relationship with Mediware Systems for the HMIS software, ServicePoint. Additionally, CCRA shall manage Agency ServicePoint End User accounts. Agency shall receive End User license(s).

(5) CCRA shall provide software implementation training. Initial training shall include agency administration, basic data entry, report generation, and data quality. Agency shall allocate paid staff time for initial training, and refresher training (#6), and End User meetings (#8).

(6) CCRA shall provide ongoing/refresher training as needed, but not less than annually, on skill enhancement and system changes.

(7) CCRA shall provide Agency with technical assistance (help desk) to access and use the HMIS. Access to basic technical assistance shall generally be available Monday through Friday from 9:00 AM - 4:00 PM based on the System Administrator's availability.

(8) CCRA shall provide Agency with End User support via coordination of End User meetings to address ServicePoint updates/product releases, data entry problems, and troubleshooting.

(9) CCRA shall develop and maintain HMIS Policies and Procedures (privacy, security, and data standards) in conjunction with the HMIS Advisory Committee.

(10) CCRA shall provide, upon request, model Privacy documents including, but not limited to, *HMIS Consumer Notice, HMIS Privacy Notice, Client Consent for HMIS Data Collection* and other templates for agreements that Agency shall adopt or adapt in implementation of the HMIS.

(11) CCRA shall audit usage and access of the HMIS.

(12) CCRA shall apply for funding to build and expand the capacity of HMIS.

II. Compliance with Privacy Rules

A. Agency represents that: **(check applicable items)**
(1) it is _____; is not _____a "covered entity" whose disclosures are restricted under HIPAA (45 CFR Parts 160 and 164). **If Agency is a "covered entity" under HIPAA, select option a or b.**

(a) _____Agency determines that substantial portion of its PPI about homeless clients or homeless individuals is protected health information as defined in the HIPAA rules. Agency that makes this determination is exempt from HMIS Privacy and Security Standards (Docket No. FR 4848-N-02).

(b)_____Agency determines that a part of Agency's operations is covered by the HMIS standards while another part is covered by the HIPAA standards. Agency that makes this determination is subject to the HMIS Privacy and Security Standards (Docket No. FR 4848-N-02).

(c) If Agency is a "covered entity" under HIPAA, Agency shall abide specifically with the *Health Insurance Portability and Accountability Act of 1996, 45 CFR Parts 160 & 164,* and corresponding regulations established by the U.S. Department of Health and Human Services. In

general, the regulations provide consumers with new rights to control the release of medical information, including advance consent of for most disclosures of health information, the right to

see a copy of health records, the right to request a correction to health records, the right to obtain documentation of disclosures of health information, and the right to an explanation of Agency's privacy rights on how information may be used or disclosed. The current regulation provides protection for electronic, paper, and oral information.

(2) it is _____; is not _____ a program whose disclosures are restricted under Federal Drug and Alcohol Confidentiality Regulations (42 CFR Part 2).

(a) If Agency is restricted under Federal Drug and Alcohol Confidentiality Regulations (42 CFR Part 2), Agency shall abide specifically by the Federal confidentiality regulations contained in *42 CFR Part 2*, regarding disclosure of alcohol and/or drug abuse records. In general terms, the federal rules prohibit the disclosure of alcohol and/or drug abuse records unless disclosure is expressly permitted by written consent of the person to whom it pertains or 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. Agency understands the federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patients.

(3) Agency shall uphold relevant federal and state confidentiality regulations and laws regarding protection of Client records.

(4) If Agency is subject to any laws or requirements which restrict Agency's ability to enter information, Agency shall ensure that any entry it makes comply with all applicable laws or other restrictions.

(5) To the extent that information entered by Agency into the HMIS is or becomes subject to additional restrictions, Agency shall immediately inform CCRA in writing of such restrictions.

(6) Agency agrees not to release any confidential information received from the HMIS to any organization or individual without proper Client consent, unless otherwise permitted by applicable laws and regulations.

(7) Agency shall comply with all HMIS Policies and Procedures pertaining to protection of Client privacy.

(8) Agency shall ensure that all staff issued User ID's and passwords to the HMIS abide by this *Partner Agency Participation Agreement*, including all associated confidentiality provisions. Agency is responsible for oversight of its own related confidentiality requirements.

B. Client Notification and Consent

(1) Agency understands it must meet the Department of Housing and Urban Development's (HUD) "Homeless Management Information Systems (HMIS) Data and Technical Standards Notice" (Docket No. FR 4848-N-02) baseline requirements for Privacy, 4.2.1 Collection Limitation, but has the option of adopting additional privacy protections that are consistent with Agency's internal operating procedures.

ServicePoint is an open system, and by participating in HMIS the Agency is to share all client data, therefore the Agency represents that:

(2) Agency shall meet the baseline requirement for consent by posting a sign, the *HMIS Consumer Notice*, at each intake desk that explains generally the reasons for collecting information. Partner Agency staff shall thoroughly explain the *HMIS Consumer Notice* to each Client. Agency shall meet baseline requirement for consent by using the HMIS *Privacy Notice* so Clients are aware of the potential uses of

their data that is given as a part of receiving services from Agency's program. Client consent of data collection shall be met by using the Universal CoC approved *Release of Information* (ROI) form to be signed by the client before data can be shared. The parent or legal guardian must provide consent for each minor in the household to share data. If a ROI is not provided by the client, their data cannot be shared. The information entered and shared will always be viewable by the HMIS participating agencies. The ROI for data sharing in HMIS does not allow an agency to release information about a client from the database. The agency must still follow their own procedures for information sharing outside HMIS.

(3) Agency shall post the *HMIS Consumer Notice* at each intake desk or comparable location that generally explains the reason for data collection. If Agency places the *HMIS Consumer Notice* in a comparable location, it must be a prominent location where it is reasonable to expect Clients to be able to read it. If client intake is not conducted in a face to face setting and the client has no visual access to a posted *HMIS Consumer Notice*, i.e. intake conducted via telephone, Agency must notify client verbally of the content within the *HMIS Consumer Notice*.

(4) The Agency shall place all *ROI* forms in a file to be located at Agency's business address and that such forms shall be made available to CCRA for periodic audits. Agency shall retain these forms for a period of 7 years after program exit, after which time the forms shall be discarded in a manner that ensures Client confidentiality is not compromised.

(5) Agency shall publish their HMIS *Privacy Notice* and provide a copy to Clients upon request. Agency's *Privacy Notice* must specify the following: 1) purposes for which Agency collects protected personal information, 2) allowable uses and disclosures, 3) Agency's *Privacy Notice* may be amended at any time and that amendments may effect information obtained by Agency before the date of change, 4) Clients' right to inspect and obtain a copy of their own personal information, 5) Clients' right to request a correction of inaccurate or incomplete personal information, and 6) Clients' right to question or complain about Agency's privacy and/or security practices. Partner Agencies must comply with all baseline privacy protections included in its *Privacy Notice*.

(6) Agency shall allow Clients to inspect and obtain a copy of their own personal information except for information compiled in reasonable anticipation of, or for use in, a civil, criminal or administrative action or proceeding.

(7) Agency shall consider any request by a Client for correction of inaccurate or incomplete personal information following Agency designated procedures. If granted, corrections shall be made by way of a new entry which is in addition to but is not a replacement for an older entry.

(8) Agency shall establish a grievance procedure for responding to Client concerns regarding use of the HMIS. The procedure shall include the following: "For Mahoning County HMIS-related grievances, a copy of the grievance and (Agency's name response) to that grievance will be forwarded to the HMIS System Administrator."

(9) Agency shall permit staff of CCRA to monitor and periodically audit its handling of confidential Client data in connection to the HMIS.

(10) Agency shall not solicit or input information from Clients into the HMIS unless it is essential to provide services or conduct evaluation or research.

(11) Agency acknowledges that ensuring the confidentiality, privacy and security of any information downloaded from the HMIS is strictly the responsibility of Agency.

(12) Agency understands the HMIS data server, which contains all Client information, is located off-site in Shreveport, Louisiana, at Mediware Systems' main office.

III. Security. Security for data maintained in HMIS depends on a secure computing environment.

(1) Agency shall allow access to HMIS only from computers which are:

a. secured by a user authentication system consisting of an End User ID and password.
b. protected from viruses by commercially available virus protection software.
c. protected with a software or hardware firewall.
d. accessed through web browsers with 128-bit encryption (e.g., Internet Explorer, version 7.0+).
e. staffed at all times when in public areas. When computers are not in use and staff are not present, steps shall be taken to ensure that the computers and data are secure and not publicly accessible. These steps shall minimally include: logging off the data entry system, shutting down the computer entirely, or physically locking the computer in a secure area.

(2) Agency shall permit staff of CCRA to monitor and periodically audit its security practices in connection to the HMIS.

IV. Data Entry and Regular Use of the Mahoning County HMIS

(1) Agency shall follow, comply with and enforce the *End User Agreement: Responsibility Statement and Code of Ethics*. Modifications to the *End User Responsibility Statement and Code of Ethics* shall be established in consultation with Partner Agencies and may be modified as needed for the purpose of the smooth and efficient operation of the HMIS.

(2) Agency shall not share assigned End User ID's and passwords to access the HMIS with any other organization, government entity, business, or individual.

(3) Agency shall enter all minimum data elements as defined for persons who are participating in services funded by the U.S. Department of Housing and Urban Development (HUD) Supportive Housing Program, Shelter + Care, Section 8 Moderate Rehabilitation for SRO, HOPWA, and Emergency Solutions Grant Program.

(4) Agency shall only enter individuals in the HMIS that exist as Clients under Agency's jurisdiction. Information entered by Agency shall be truthful, accurate, and complete to the best of Agency's knowledge. Agency shall not misrepresent its Client base by entering known, inaccurate information.

(5) Agency shall consistently enter information into the HMIS. Agency shall routinely review records it has entered into the HMIS for completeness and accuracy.

(6) Agency shall use Client information in the HMIS to assist Agency in providing adequate and appropriate services to Clients.

(7) Agency shall use the HMIS for business purposes only.

(8) Agency shall not use the HMIS with the intent to defraud federal, state or local governments, individuals or entities, or to conduct illegal activity.

(9) Agency shall not enter offensive language, profanity, or discriminatory comments based on race, color, religion, national origin, ancestry, handicap, age, sex, and sexual orientation in the Mahoning County HMIS.

(10) The transmission of material in violation of any federal or state regulations is prohibited. This includes, but is not limited to, copyright material, material legally judged to be threatening or obscene, and material considered protected by trade secret.

V. Reports

(1) Agency shall retain access to identifying and statistical data on Clients it serves. Agency may release Agency's data to other entities for public relations, reporting, funding, and planning purposes. However, such data shall not directly or indirectly identify individual Clients.

(2) Agency understands that when it enters information into the HMIS, such information will be available to CCRA staff who shall review data to administer the HMIS, to conduct analysis, and to prepare reports.

(3) CCRA shall only use de-identified, aggregate (not Agency specific) HMIS data for homeless policy and planning decisions, in preparing for federal, state, or local applications for homelessness funding, to demonstrate the need for and effectiveness of programs, and to obtain a system -wide view of program utilization in the county. Agency hereby authorizes CCRA to include Agency's data in reports.

(4) CCRA shall publish community-wide aggregate HMIS homeless data (not Agency specific). These reports shall be raw point-in-time data. Public reports will not be released until the Mahoning County Continuum of Care is comfortable with the reliability of the data. Agency may use published HMIS data.

(5) CCRA shall never release proprietary information about Agency, its services, procedures, or Client demographics without written permission of Agency. CCRA shall only release Agency-specific data with permission of Agency.

(6) Agency understands that CCRA and the Mahoning County Continuum of Care HMIS Advisory Committee shall further develop policies and procedures concerning the use and release of aggregate system- wide data.

VI. Proprietary Rights of Mediware Systems

(1) Agency shall not give or share assigned ServicePoint passwords and access codes of the Mahoning County HMIS with any other Agency, business, or individual.

(2) Agency shall take due diligence not to cause in any manner, or way, corruption of the HMIS ServicePoint database. Any unauthorized access or unauthorized modification to computer system information, or interference with normal system operations, shall result in immediate suspension of services, and where appropriate, legal action against the offending entity. Agency agrees to be responsible for any damage it may cause.

VII. Hold Harmless

A. Disclaimer of Warranties

(1) CCRA makes no warranties, expressed or implied.

B. Limitation of Liability and Indemnification

(1) Generally, no party to this Agreement shall assume any additional liability of any kind due to its execution of this agreement of participation in the HMIS. It is the intent of the parties that each party shall remain liable, to the extent provided by law, regarding its own acts and omissions; but that no party shall assume additional liability on its own behalf or liability for the acts of any other person or entity except for the acts and omissions of their own employees, agents, or contractors through participation in the HMIS. The parties specifically agree that this agreement is for the benefit of the parties only and this agreement creates no rights in any third party.

(2) Specifically, Agency, at all times, shall indemnify and hold CCRA harmless from any damages, liabilities, claims, and expenses that may be claimed against Agency; or for injuries or damages to Agency or another party arising from participation in the HMIS; or arising from any acts, omissions, neglect, or fault of Agency or its agents, employees, licensees, or Clients; or arising from Agency's failure to comply with laws, statutes, ordinances, or regulations applicable to it or the conduct of its business. Agency shall also hold CCRA harmless for loss or damage resulting in the loss of data due to delays, non-deliveries, mis-deliveries, or service interruption caused by Mediware Systems, by Agency's or other

member agency's negligence or errors or omissions, as well as natural disasters, technological difficulties, and/ or acts of God. CCRA shall not be liable to the Agency for damages, losses, or injuries to the Agency or another party other than if such is the result of gross negligence or willful misconduct of CCRA. CCRA shall hold Agency harmless from any damages, liabilities, claims or expenses caused solely by the negligence of CCRA.

(3) The Provisions of Section VII shall survive any termination of this *Partner Agency Participation Agreement.*

VIII. Terms and Conditions

(1) Agency shall abide by such guidelines as are promulgated by HUD and/or CCRA from time to time regarding administration of the HMIS.

(2) This agreement shall be governed by and construed in accordance with the laws of the State of Ohio, and only Ohio courts shall have jurisdiction in any action brought against CCRA.

(3) Neither CCRA nor Agency shall transfer or assign any rights or obligations under the *Partner Agency Participation Agreement* without the written consent of either party. Neither Agency's right to participate in the HMIS nor any other right, privilege, license, duty, obligation, or responsibility may be transferred or assigned, voluntarily or involuntarily, through agreement, merger, consolidation, or otherwise without the express written consent of CCRA.

(4) This agreement may be modified or amended by written agreement executed by both parties with 30 days advance written notice.

(5) This agreement shall remain in force until revoked in writing by either party, with 30 days advance written notice. The exception to this term is if allegations or actual incidences arise regarding possible or actual breaches of this agreement. Should such situations arise, CCRA may immediately suspend access to the HMIS until the allegations are resolved in order to protect the integrity of the system.

Signatures

I agree to abide by the system policies and procedures outlined above concerning Agency participation in the Mahoning County HMIS.

_____ _____

Signature of Executive Director, HMIS Lead Agency Date

I request implementation of the Mahoning County HMIS and use of ServicePoint software for my Agency. I agree to abide by all system policies and procedures outlined above.

_____

Agency Name

_____

Print Name of Executive Director

_____ _____

Signature of Executive Director Date

ATTACHMENT C

MahoningCounty HMIS
SECURITY OFFICER AGREEMENT

For: _____
Agency Name

The following signature constitutes an understanding and agreement that the person designated by the HMIS Partner Agency documented below shall abide by the following statements and responsibilities which are published in the Mahoning County HMIS Policies and Procedures Manual. The HMIS Security Officer is the primary contact at the HMIS Partner Agency. The Security Officer provides a single point of communication between End Users and the HMIS System Administrator. The Security Officer is responsible for:

(1) Ensuring access to ServicePoint is granted to authorized staff only after they have received training and executed a *HMIS End User Agreement: Responsibility Statement and Code of Ethics*. Need exists only for those staff who work directly with (or supervise staff who work directly with) Clients or have data entry responsibilities.

(2) Enforce business controls and practices to ensure organizational adherence to the Mahoning County HMIS policies and procedures, and HUD Data and Technical Standards, including the following:
-monitoring compliance with standards of Client confidentiality and ethical data collection, entry, and retrieval.
-ensuring completeness and accuracy of client-level data entered into the HMIS.
-monitoring and taking appropriate action if misuse of ServicePoint occurs.

(3) Provide support for the generation of agency reports, including the HUD APR.

(4) Ensure the stability of the agency connection to the Internet and ServicePoint, either directly or in communication with other technical professionals, including network firewall updates and maintenance, password protection, virus software updates and maintenance, as well as any other related privacy and security issues to ensure client confidentiality is protected as outlined in the policies and procedures manual.

_____
Print Name of Security Officer

_____ _____
Signature of Security Officer Date

_____ _____

Signature of Executive Director Date

ATTACHMENT D

Mahoning County HMIS

END USER AGREEMENT: RESPONSIBILITY STATEMENT AND CODE OF ETHICS

For: _____

Agency Name *(please print)*

This Agency recognizes the primacy of Client needs in the design and management of the Mahoning County Homeless Management Information System (HMIS). These needs include both the need to continually improve the quality of homeless and housing services with the goal of eliminating homelessness in Mahoning County, and the need to vigilantly maintain Client confidentiality, treating the protected personal information of our most vulnerable populations with respect and care.

As the guardians entrusted with this protected personal information, HMIS End Users have an ethical and a legal obligation to ensure that the data they collect is being collected, accessed, and used appropriately. It is also the responsibility of each End User to ensure that Client data is only used to the ends to which it was collected and ends that have been made explicit to Clients. Proper End User training, adherence to the Mahoning County HMIS Policies and Procedures Manual, and a clear understanding of Client confidentiality are vital to achieving these goals.

User Responsibility

Your ServicePoint End User ID and password give you access to the HMIS. **Initial each item below to indicate your understanding of proper access to the HMIS.** Failure to uphold the security and confidentiality standards set forth below is grounds for immediate termination from the HMIS and may result in disciplinary action from the HMIS Partner Agency as defined in the Partner Agency's personnel policies.

I agree to maintain the confidentiality of Client information in HMIS in the following manner:

(1) _____ I shall only view, obtain, disclose, or use HMIS information that is necessary to perform my job.

(2) _____ I understand that the only individuals who may directly access HMIS Client information are authorized users, and I shall take these steps to prevent casual observers from seeing or hearing HMIS Client information.

(3) _____ My End User ID and password are for my use only and I shall not share them with anyone.

(4) _____ My password shall be at least 8 characters long and meet reasonable industry standard requirements as specified in the HMIS Policies and Procedures Manual.

(5) _____ I shall take reasonable means to keep my password physically secure.

(6) _____ I shall limit physical access to my HMIS workstation by setting a password protected screensaver or employing auto-log.

(7) _____ I shall not leave my HMIS workstation unattended when ServicePoint is open and

running.

(8) _____ I shall log off of ServicePoint before leaving my work area or make sure that the ServicePoint has "timed out" before leaving my work area.

(9) _____ I shall store hard copies of HMIS information in a secure file and not leave such hard copy information in public view on my desk, or on a photocopier, printer or fax machine.

(10) _____ I shall properly destroy hard copies of HMIS information when they are no longer needed unless they are required to be retained in accordance with applicable law.

(11) _____ I understand that a failure to follow these security steps appropriately will result in a breach of HMIS Client confidentiality. If such a breach occurs, my access to the HMIS may be terminated and I may be subject to further disciplinary action as defined in the HMIS Partner agency's personnel policy.

(12) _____ If I notice or suspect a security breach, I shall immediately notify the Executive Director of my Agency and the HMIS System Administrator.

(13) _____ I understand that HMIS is an open system sharing data with all participating agencies and as such I must verify that the universal Mahoning County HMIS Release of Information form has been signed by every client prior to my entering the client into the system. If a client does not have a Release of Information signed, it is my responsibility to close the client record upon creation of information in the system to ensure that there is not a breach of confidentiality or security.

By executing this agreement, you agree to abide by the following Client confidentiality provisions:

(1) I shall maintain HMIS data in such a way as to protect against revealing the identity of Clients to unauthorized agencies, individuals, or entities.

(2) I shall keep confidential information obtained from the HMIS confidential, even if my relationship with this Agency changes or concludes for any reason.

(3) I shall not deny Clients or potential Clients service for failure to provide consent for HMIS data collection.

(4) I shall faithfully respect Client preferences with regard to the entry of Client information within HMIS.

(5) I shall observe the HMIS Client consent policy and client consent option this Agency designated as to comply with.

(6) I shall allow Clients to revoke consent upon written request.

(7) I shall allow Clients to inspect, copy, and request changes to the Clients' own information maintained within HMIS upon written request. Information compiled in reasonable anticipation of or for use in a civil, criminal or administrative action or proceeding need not be provided to Client.

(8) I shall permit Clients to file a written complaint regarding the use or treatment of their information within the HMIS. Clients may file a written complaint with the Agency. The Client may not be retaliated against for filing a complaint.

(9) Information I enter into the HMIS shall be truthful, accurate and complete to the best of my knowledge. I acknowledge that misrepresentation of the Client base by entering known, inaccurate information is prohibited. Any information that is not given by the Client should be left blank.

User Code of Ethics

(1) I shall maintain high standards of professional conduct in my capacity as an HMIS End User.

(2) I shall endorse and maintain the Client's rights related to privacy and confidentiality and shall adhere to HMIS Policies and Procedures.

(3) I shall not solicit from or enter information about Clients into the HMIS unless the information is required for a legitimate business purpose such as to provide services to the Client.

(4) I shall not use the HMIS system with intent to defraud the federal, state, or local government; an individual entity; or to conduct illegal activity.

(5) I shall not enter discriminatory comments based on race, color, religion, national origin, ancestry, handicap, age, sex, and sexual orientation in the HMIS system.

(6) Transmission of material in violation of any United States Federal or State of Ohio regulations or laws is prohibited and includes material that is copyrighted, and/or legally judged to be threatening or obscene.

I affirm the following:

(1) I have received training in how to use the HMIS.
(2) I have read and will abide by all policies and procedures in the Mahoning County HMIS Policies and Procedures Manual.
(3) I will maintain the confidentiality of Client data in the HMIS as outlined above and in the Mahoning County HMIS Policies and Procedures Manual.
(4) I acknowledge receipt of the *Privacy Notice* and pledge to conform with all standards contained therein.
(5) I will only collect, enter, and extract data in the HMIS that is relevant to the delivery of services to people experiencing homelessness in Mahoning County.

The signature below indicates an agreement to comply with this statement of confidentiality.

_____
Print Name of HMIS End User

_____ _____
Signature of HMIS End User Date

_____ _____
Signature of Executive Director Date

Mahoning County HMIS
Authorization for the Release of Information
_____Effective October 1, 2014_____

Purpose for Data Collection
The information gathered will be shared with HMIS Participating Agencies in a HMIS database and shall be used to more effectively:

(1) Provide individual case management
(2) Monitor the outcomes of services that are provided to you
(3) Identify unfilled service needs and plan for the provision of new services
(4) Improve the quality of care and services for homeless individuals and families
(5) Produce anonymous, aggregate-level reports regarding use of services

Information to be Released
By signing below you consent to share the following information, including all historical information collected and entered into HMIS prior to this date. A list of HMIS Participating Agencies is available upon request.

HUD CoC and ESG Assessment and PATH Assessment Data Elements
Includes: Name, Alias, Photo, Social Security Number, and Social Security Data Quality, Date of Birth, Gender, Primary Race, Secondary Race, Ethnicity, Homeless Status, Housing Status, Chronically Homeless Status, Residence Prior to Entry, Length of Stay, Veteran Status, Domestic Violence Victim, Length of Domestic Violence, Disabling Condition, Disability Type, Disability Start and End Dates, If the Disability will be Long Term, if the Client is Receiving Treatment for the Disability, Total Monthly Income, Income Type, Income Amount, Income Start and End Dates, Non Cash Benefits, Non Cash Benefits Source, Non Cash Benefits Start and End Dates, Health Insurance, Health Insurance Source, Health Insurance Start and End Dates, Date of Engagement and How the Client was Contacted, Entry Date, Program Name, Household Members Related to the Program Entry, Exit Date, Destination, and Reason for Leaving, Program Specific Services Provided by your Program, Program Name, Service Start and End Dates, and Household Member with Related Services.

This information has been disclosed from records protected by Federal confidentiality rules (42 CFR part 2). The Federal rules prohibit you from making any further disclosure of this information unless further disclosure is expressly permitted by the 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 federal rules restrict any use of the information to criminally investigate or prosecute any alcohol or drug abuse patient.

I understand that I have the right to inspect, copy, and request all records maintained by the Agency relating to the provision of services to me. I understand that I may revoke this consent at any time. I further understand that this consent is subject to revocation at any time, except to the extent that the Agency has already taken action in reliance on it. Additionally, I understand that participation in data collection is optional, and I am able to access shelter, housing, and/or support services if I choose not to participate in data sharing. This consent expires one year from the date of signature.

_____

Client Name (please print) Signature Date

_____

Guardian Name, if applicable (please print) Guardian Signature Date

Mahoning County HMIS

PRIVACY NOTICE

This *Privacy Notice* describes how information about you may be used and disclosed in the Mahoning County Homeless Management Information System (HMIS) and how you can get access to this information. Please review it carefully. The privacy of your personal information is important to us.

Purpose of This Notice
This *HMIS Privacy Notice* tells you about how we use and disclose your protected personal information. It tells you about your rights and our responsibilities to protect the privacy of your protected personal information. It also tells you how to complain to us if you believe that we have violated any of your rights or any of our responsibilities.

We are required by law to maintain the privacy of your protected personal information. We must provide you with a copy of this *HMIS Privacy Notice* upon request. We must follow the terms of this Notice that are currently in effect.

We reserve the right to change our privacy practices and terms of this *HMIS Privacy Notice* at any time, provided such changes are permitted by applicable law. If this Notice is changed, a copy of the revised notice will be available upon request. The new terms shall be effective for all protected personal information that we maintain, including information we created or received before we made the changes.

What is the Mahoning County Homeless Management Information System?
In order to best serve your needs, we enter information about you and members of your family that are with you into a computer system called the Mahoning County HMIS. The HMIS is used by many homeless providers in Mahoning County that provide shelter, housing, and related support services. Although the HMIS helps us to keep track of your information, individually identifiable information about you is considered "Protected Information". Please, understand that access to shelter and housing services is available without your participation in data collection. However, your participation, although optional, is a critical component of our community's ability to provide the most effective services and housing possible.

Why is information about you collected in the Mahoning County HMIS?

(1) To provide individualized case management and help make sure you get services you need.
(2) To help us better understand the people we serve and their needs.
(3) To help us understand the types of services people need and develop new services to meet the unmet needs.
(4) To monitor whether your needs, and the needs of others in our community, were met.

(5) To improve the quality of care and service for homeless individuals and families.

How We Use or Disclose Your Private Personal Information.
Unless restricted by other laws, your information can be used by or disclosed to the following without your specific written consent:

(1) To provide or coordinate services. We will use protected personal information about you to provide you with services. Upon a signed Release of Information from you, we will share this information with members of our staff and with others involved in your support. This includes other homeless services providers participating in the HMIS system. We will also use your protected personal information for functions related to payment or reimbursement for services.
(2) To carry out administrative functions of our office. We will use and disclose your private personal information for operational purposes. For example, we may use your private personal information to evaluate our services, including the performance of our staff in caring for you. We may also use this information to learn how to continually improve the quality and effectiveness of the services that we provide to you. This also includes auditors or others who review the work of this Agency or need to review the information to provide services to this Agency.
(3) Mahoning County HMIS System Administrator. The HMIS System Administrator runs the computer system to maintain the data. The SA will see your information in the process of fixing problems, running reports, or testing the system.

Other Uses or Disclosures of Your Personal Information
Unless restricted by other laws, your information can be used by or disclosed to the following without your specific written consent:

(1) Required by Law. We may disclose protected personal information about you when required by law to the extent that the use or disclosure complies with and is limited to the requirements of the law.
(2) Public Health Activities. We may disclose private personal information about you if the HMIS user or developer, in good faith, believes that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public and is made to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat.
(3) Funeral Directors, Coroners, and Medical Examiners. We may disclose protected personal information about you as necessary to allow these individuals to carry out their responsibilities.
(4) Victims of Abuse, Neglect or Domestic Violence. We may disclose protected personal information about you to a government agency if we believe you are the victim of abuse, neglect or domestic violence.
(5) Academic Research Purposes. We may disclose protected personal information about you to staff from the sponsoring organizations or other authorized individuals who have permission to do research or report on the use and effectiveness of the services provided to you and others.
(6) Legal Activities and Law Enforcement. We may disclose protected personal information about you to law enforcement officials for law enforcement purposes:
    a. As required by law;
    b. In response to a court order, subpoena or other legal proceeding;
    c. To identify or locate a suspect, fugitive, material witness or missing person;
    d. When information is requested about an actual or suspected victim of a crime;
    e. To report a death as a result of possible criminal conduct;
    f. To investigate allegations of misconduct that may have occurred on our premises;
    g. To report a crime in emergency circumstances.

(7) National Security and Intelligence. We may disclose protected personal information about you to authorized federal officials for national security and intelligence activities.
(8) Protective Services for the President and Others. We may disclose protected personal information about you to authorized federal officials for the provision of protective services to the President of the United States or other foreign heads of state.

Uses or Disclosures That Require Your Authorization
Other uses and disclosures will be made only with your written consent. You may cancel your consent at any time in writing. Once consent is given, your information may be released until such time as the cancellation is received and made known to those with authorized access.

What rights are your rights regarding your information?
The information contained in your HMIS record maintained by *(insert Agency name)* are the physical property of *(insert Agency name)*. The information in it belongs to you. You have the following rights:

(1) You have the right to an explanation of any information contained in this *HMIS Privacy Notice* that you may not fully understand.
(2) You have the right to obtain a copy of this *HMIS Privacy Notice* and any revisions we make to the Notice at any time.
(3) You have the right to inspect and obtain a copy of the information that we maintain about you in the Mahoning County HMIS except for information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.
(4) You have the right to request a correction of information that we maintain about you in the Mahoning County HMIS that you believe to be inaccurate or incomplete. You can exercise your rights as listed above by making a written request to *(insert Agency name)* at *(insert Agency address)*.
(5) You have the right to question or complain about *(insert Agency name)* privacy and/or security policies and practices. If you believe that your privacy rights have been violated, you may send a written complaint to *(insert Agency name)* at *(insert Agency address)*. We are prohibited from retaliating against you for filing a complaint.

If you have further questions about this *HMIS Privacy Notice* or about your rights, contact *(insert Agency name)* at *(insert Agency telephone number)*. Please note, however, that *(insert Agency name)* cannot provide specific legal advice to you regarding your rights.

Greivance Procedures
For MahoningCounty HMIS-related grievances, a copy of the grievance and *(Agency's name)* response to that grievance will be forwarded to the HMIS System Administrator. Partner Agencies are obligated to report all HMIS-related grievances to the HMIS System Administrator, who documents and summarizes all grievances and resolutions. This information is made available to the HMIS Advisory Committee to determine the need for further action, if any. These actions might include further investigation of incidents, clarification or review of policies, or sanctioning of HMIS End Users and agencies if End Users or agencies are found to have violated standards set forth in HMIS Agency Agreements or the Policies and Procedures Manual.

Mahoning County HMIS

CONSUMER NOTICE

This Agency receives funding from U.S. Department of Housing and Urban Development to provide services for homeless and near homeless individuals and their families. A requirement of this funding is participation in the Mahoning County Homeless Management Information System (HMIS). This requirement was enacted to produce an accurate count of individuals and families who are homeless, to better understand the needs of our clients, and to improve our services.

We only collect information that we consider to be appropriate. The collection and use of all personal information is guided by strict standards of confidentiality. A copy of our *Privacy Notice*

describing our privacy practice is available to all consumers upon request.

Public Notice (Federal Register / Vol. 69, No. 146) / Effective August 30, 2004

APPENDIX A: DATA ELEMENTS
UPDATED JUNE 2016

UNIVERSAL
1. NAME
2. SOCIAL SECURITY NUMBER
3. DATE OF BIRTH
4. RACE
5. ETHNICITY
6. GENDER
7. VETERAN STATUS
8. DISABLING CONDITION
9. RESIDENCE PRIOR TO PROJECT ENTRY
10. PROJECT ENTRY DATE
11. PROJECT EXIT DATE
12. DESTINATION
13. PERSONAL IDENTIFICATION NUMBER
14. HOUSEHOLD IDENTIFICATION NUMBER
15. RELATIONSHIP TO HEAD OF HOUSEHOLD
16. CLIENT LOCATION
17. LENGTH OF TIME HOMELESS

PROGRAM-SPECIFIC DATA ELEMENTS
1. HOUSING STATUS
2. INCOME AND SOURCES
3. NON-CASH BENEFITS
4. HEALTH INSURANCE
5. PHYSICAL DISABILITY
6. DEVELOPMENTAL DISABILITY
7. CHRONIC HEALTH CONDITION
8. HIV/AIDS
9. MENTAL HEALTH PROBLEM
10. SUBSTANCE ABUSE
11. DOMESTIC VIOLENCE
12. CONTACT
13. DATES OF ENGAGEMENT AND ENROLLMENT
14. VETERANS INFORMATION
15. SERVICES PROVIDED
16. FINANCIAL ASSISTANCE PROVIDED

17. HOUSING ASSESSMENT AT EXIT
18. PATH STATUS
19. CONNECTION WITH SOAR
20. BCP STATUS
21. SEXUAL ORIENTATION
22. LAST GRADE COMPLETED
23. SCHOOL STATUS
24. GENERAL HEALTH STATUS
25. EMPLOYMENT STATUS
26. PREGNANCY STATUS
27. REFERRALS PROVIDED
28. REASON FOR LEAVING
29. FORMERLY A WARD OF CHILD WELFARE / FOSTER CARE AGENCY
30. FORMERLY A WARD OF JUVENILE JUSTICE SYSTEM
31. YOUNG PERSON'S CRITICAL ISSUES
32. REFERRAL SOURCE
33. COMMERCIAL SEXUAL EXPLOITATION
34. COMMERCIAL LABOR EXPLOITATION
35. TRANSITIONAL, EXITCARE, OR AFTERCARE PLANS AND ACTIONS
36. PROJECT COMPLETION STATUS
37. FAMILY REUNIFICATION ACHIEVED
38. DENTAL HEALTH STATUS
39. MENTAL HEALTH STATUS
40. MEDICAL ASSISTANCE
41. T-CELL (CD4) AND VIRAL LOAD
42. PERCENT OF AMI
43. LAST PERMANENT ADDRESS
44. HP SCREENING SCORE
45. VAMC STATION NUMBER