E.1

HOMELESS CONTINUUM OF CARE OF STARK COUNTY HOMELESS MANAGEMENT INFORMATION SYSTEM (HMIS) POLICY

PURPOSE: Enhance the ability to collect accurate data and to provide guidance for the efficient administration, implementation, and maintenance of the HMIS system that meets HUD requirements.

The Homeless Continuum of Care of Stark County (hereinafter HCCSC) recognizes that Participant needs must drive the HMIS design and management. The HCCSC will use the HMIS to pursue its goals to eliminate homelessness in our community and to improve the quality of homeless and housing services.

As the guardians entrusted with this personal data, HMIS Users have a moral and a legal obligation to ensure that the data they collect is accessed and used appropriately. Each User is responsible to ensure that Participants data is only used to accomplish the HCCSC goals. Users must ensure Participants understand how the data will be used and that the data use is consistent with the mission to assist families and individuals resolve their housing crises.

Proper user training, adherence to the HMIS Policies and Procedures Manual, and a clear understanding of Participant confidentiality are vital to achieving these goals.

SECTION I
ROLES AND RESPONSIBILITIES

Policy: The HCCSC is responsible for approving HMIS policies and procedures that comply with HUD requirements, monitoring compliance with HMIS policies, and assembling an HMIS Committee. In compliance with HUD requirements and to ensure the effective and efficient implementation and use of the HMIS, specific roles and responsibilities will be assigned to the HMIS Committee, the Lead HMIS Agency, the HMIS Administrator and HMIS Agency Staff.

1.01 Lead HMIS Agency

Procedure:

1. The Lead HMIS Agency shall be appointed by the HCCSC and will enter into a Memorandum of Agreement (MOA) with the HCCSC.

2. The HMIS Administrator shall be an employee of the Lead HMIS Agency.

1.02 HCCSC HMIS Committee

Procedure:

1. HCCSC will assemble an HCCSC HMIS Committee (hereinafter HMIS Committee), and appoint the chair(s) of the Committee, that will guide the administration of HMIS policy and monitor provider compliance. The HMIS Committee will include, but is not limited to:
    - An HCCSC representative;
    - HMIS Administrator;
    - HMIS Participating Agencies;
    - key stakeholders;
    - and where possible, persons with knowledge or expertise in data design, collection, and systems administration.

2. HMIS Committee will meet on a routine basis as defined by the Committee to review and recommend HMIS policies, plan for training, troubleshoot system problems, monitor secure software access, and provide feedback to the HMIS Administrator and HMIS Participating Agencies.
3. HMIS Committee is responsible for drafting new procedures, reviewing existing procedures and problems raised during implementation of existing policies, and making recommendations on policies to adopt or change. HMIS Committee will revise or create policies as needed and will forward them to HCCSC for final approval. All policies and procedures will comply with HUD requirements.
4. The HMIS Committee will oversee protocols and assist with HMIS CoC issues.
5. The HMIS Committee will develop and review policies for customized data reports (including frequency, notice, level of customization, allowable data, and other related items) and recommend a cost structure for additional non-mandatory reports as requested by HCCSC.
6. HMIS Committee will oversee data reports on Participating Agencies to monitor data quality.
7. The HMIS Committee may form an HMIS Advisory Group with the explicit purpose of resolving any specific issue(s). After issue(s) has/have been resolved Group may be dissolved. The Advisory Group will include users and facilitators with technical expertise.

1.03 HMIS Staff

Procedure:

1. The HMIS Administrator or designee will coordinate and administer the HMIS including data collection, data entry of primary HMIS data, connectivity, and reporting of compliance or other data issues.
2. The HMIS Administrator will keep a list of all agencies (i.e., Participating Agencies) and agency staff (i.e., HMIS Users) authorized to use the HMIS.

1.04 HMIS Administrator

Procedure:

1. The HMIS Administrator has access to retrieve all data in the HMIS and will facilitate retrieving individual records of multiple social service programs, primarily those that serve the homeless.
2. The HMIS Administrator may provide aggregate data reports to all authorized requestors and -system specific reports to each Agency regarding their own data.
3. The HMIS Administrator will monitor HMIS level data collection and HMIS main system data entry.
4. The HMIS Administrator is also responsible for generating aggregated data reports.
5. The HMIS Administrator may designate others within the lead HMIS agency to fulfill these functions as s/he determines.

SECTION II
PARTICIPATING AGENCIES

Policy: Participating Agencies shall be required to comply with all HUD and HMIS requirements. Participating Agencies shall assign specific internal roles, establish and implement internal processes necessary for proper HMIS functionality and compliance, and follow HMIS communication protocols.

2.01 Participating Agencies - Agency Administrators

Procedure:

1. Each Participating Agency will designate an HMIS Agency Administrator who will serve as the primary liaison with the HMIS Administrator and who will be responsible for monitoring agency compliance and data quality. Each Participating Agency must have a designated HMIS Agency Administrator at all times. If no administrator has been appointed to the HMIS Administrator, the

Agency's Executive Director (or Chief Executive Officer) shall serve as the Agency HMIS Administrator.

2. The Agency HMIS Administrator will be the primary contact person and provide their contact information to the HMIS Administrator and the HMIS Committee, including changes such as replacement contact information or changes in contact names, addresses or numbers.
3. The HMIS Agency Administrator (or other empowered officer) of Participating Agencies will sign an HMIS Agency Partner Agreement (see document E.2).

2.02 Participating Agencies

Procedure:

1. Participating Agencies shall abide by all Policies and Procedures outlined and referenced herein and the requirements of the Agency Partner Agreement, HCCSC HMIS Privacy Notice (see document E.4), Data Quality Plan (see document E.6), and Security Plan (see document E.5).
2. Participating Agencies shall designate who will have access to the HMIS in their respective agencies (i.e., their HMIS Users).
3. Participating Agencies will conduct a background check on each of their designated HMIS Users and will take all necessary steps to ensure that the designated users understand and abide by HMIS Policies as stated herein.
4. Participating Agencies that are noncompliant with HMIS Policies may lose the right to access HMIS directly. They may also be billed for expenses incurred by the HMIS Administrator for entering and/or retrieving data on their respective Agency's behalf.
5. Participating Agencies shall inform the HMIS Administrator in writing within one business day of changes in the Agency's authorization of HMIS Users.
6. Participating Agencies shall require each member of its staff (including employees, volunteers, affiliates, contractors and associates) to sign a Stark County HMIS User Agreement that acknowledges receipt of a copy of the Participating Agency's privacy notice and that pledges to comply with the privacy notice.

2.03 Participating Agency Hardware/Software Requirements

Procedure:

1. Connection to the HMIS requires a broadband connection approved by the HMIS Administrator or designee.

2. Operating software must meet the specifications required by the HMIS Software Vendor.

2.04 Participating Agency Technical Support Requirements

Procedure:

Participating Agencies are responsible for providing their own technical support for all hardware and software systems used to connect to the HMIS. Agencies are responsible for maintaining connectivity to the HMIS.

2.05 HMIS Users

Procedure:

1. Each Participating Agency staff member who has access to the HMIS (i.e., HMIS User) will sign a Stark County HMIS User Agreement authorizing her/his use of the HMIS.
2. Only staff members authorized by the HMIS Agency Administrator as HMIS Users shall be permitted to access the HMIS.
3. The right to use the HMIS terminates when a staff member identified as an HMIS User leaves the Participating Agency for any reason, or changes positions where use of the HMIS is no longer part of the staff member's responsibilities.
4. HMIS Users shall comply with the confidentiality requirements of Section VI of this policy, the HMIS Privacy Notice and the HMIS User Agreement.
5. HMIS Users shall ensure that individual Participant data contained in the HMIS is only shared with agencies that are specified in the HMIS Participant Informed Consent and Release of Information Authorization.
6. HMIS Users will secure HMIS data to protect against revealing the identity of Participants to unauthorized agencies, individuals, or entities in accordance with the HMIS Security Plan.
7. Any HMIS User found to be in violation of the HMIS Policies and Procedures, or the points of Participant confidentiality in the User Agreement, may be denied access to the HMIS.

2.06 HMIS User Access Levels

Procedure:

The HMIS Committee will seek the HMIS Administrator's recommendations to determine appropriate HMIS security access levels. Agency Administrators are

responsible for determining appropriate levels of access to the HMIS data for each of their users.

2.07 Communication with Participating Agencies

Procedure:

1. Each Participating Agency shall appoint one primary contact for all global communications.
2. The HMIS Administrator or designee may contact either the HMIS Agency Administrator or User directly to discuss data discrepancies or to respond to a request for assistance with a specific issue or problem.
3. Participating Agencies will report problems to the HMIS Administrator. If the issue is not resolved, the Agency may seek resolution from the HMIS Committee. Final resolution may be solicited from HCCSC after all other options have been exhausted.

2.08 System Availability

Procedure:

1. Participating Agencies will promptly report HMIS system problems to the HMIS Administrator in writing.
2. The HMIS Administrator will contact the Approved Software Vendor to deal with systems issues.
3. The HMIS Administrator will inform Participating Agencies in advance of any planned interruption in service and will communicate details and remedies when unplanned interruptions occur.
4. In the event the Approved Software is not available, Participating Agencies will collect data manually until it is reconnected and can enter the information into the system.

2.09 HMIS User Licenses

Procedure:

Participating Agencies may be allowed additional User licenses with approval from the HMIS Administrator provided that the need to add Users is consistent with the Purpose Statement of this Policy as stated herein. Cost of additional User licenses may be passed on to the requesting Agency.

2.10 HMIS User Activation

Procedure:

Each new User will be issued a username and password to access the HMIS. Permission is granted after the new User has had appropriate training and has signed the HMIS User Agreement.

2.11 Training

Procedure:

The HMIS Administrator or designee is responsible for providing the initial HMIS training. Participating Agencies that have frequent changes in Users may be charged for additional trainings.

SECTION III
DATA COLLECTION

Policy: HMIS Data shall be collected and maintained in a manner that ensures the accuracy, appropriateness, integrity and usefulness of the data, in compliance with HUD requirements and the HMIS Data Quality Plan.

3.01 Required Data Collection

Procedure:

1. Data shall only be collected and maintained for the limited purposes stated in the HSSCS HMIS Privacy Notice.
2. All HCCSC service providers shall collect all HUD, State, County, City, HCCSC, or other funder required Participant data.
3. The required data elements are specified in the HMIS database.
4. Participating Agencies shall provide and/or enter into the HMIS the required set of data variables for each Participant. The HMIS Administrator shall designate an individual or other Participating Agency to enter the required data on behalf of those Participating Agencies that do not do direct data entry.
5. Victim service providers are prohibited from entering data into the HMIS.

3.02 Appropriate Data Collection

Procedure:

Users may collect additional data relevant to the delivery of services.

3.03 Data Integrity

Procedure:

All HMIS Users are responsible for the accuracy, timeliness and completeness of their data entry.

3.04 Data Integrity Expectations

Procedure:

All Users are expected to exercise diligence in gathering and entering data. All Users who have repeated data entry problems will receive additional training. Chronic problems may be reported to the HMIS Committee. If problems are unresolved, problems may be elevated to the HCCSC Board per the HMIS Data Quality Plan.

3.05 Data Corrections

Procedure:

1. Each Participating Agency that reviews individual level data shall assist in confirming HMIS information is accurate and up-to-date, based on information gained through direct contact with Participants and review documents such as driver's license, social security card, birth certificate, attendance records, or other credible documents.
2. Participating Agencies shall report data errors to the HMIS Administrator within five working days of finding an error.
3. Within five working days of receipt, the HMIS User at the Participating Agency will either correct the error or provide supporting documentation. HMIS Administrator will have final decision-making authority.

3.06 Data Element Customization

Procedure:

1. The HMIS Software does not allow for agency-specific customization of Participant data fields. Agency-specific customization is available for agency

program information.

2. Agencies may submit a request for modification of the HMIS software to the HMIS Administrator. The decision to make a modification will consider the benefit to all HMIS Users, cost, how the modification will be paid for, and agreement by the Software Provider. The HMIS Administrator will inform HMIS Committee about modifications but does not need its authority to make the change.

3.07 Agency Review Process

Procedure:

The HMIS Administrator will conduct onsite reviews as needed. Participating Agencies may be charged for costs of additional reviews needed to resolve chronic problems.

3.08 Data Outcomes

Procedure:

Outcomes performance reports are provided to the appropriate committees by the HMIS administrator.

3.09 Data Retention

1. Stark County HMIS only collects personal information that is relevant to the purposes for which it is planned to be used (see HMIS Privacy Notice for full list of information collection purposes and uses of information). To the extent necessary for those purposes, Stark County HMIS seeks to maintain only personal information that is accurate, complete, and timely.

The disposal of personal information not in current use will occur when there is an HMIS version update and will not exceed seven years after the information was last changed.

2. Personal information may be kept for a longer period if required to do so by statute, regulation, contract, or other requirement.

SECTION IV
ACCESS TO HMIS

Policy: User Access to HMIS shall be controlled through implementation of processes that ensure the confidentiality and security of the system and the data.

4.01 HMIS User Access

Procedure:

1. The HMIS Administrator creates and assigns all initial usernames and passwords.
2. HMIS database usernames and passwords shall be unique and may not be shared or exchanged with other Users, unless authorized by the HMIS Administrator.
3. Only the HMIS Administrator or designee will have access to the list of HMIS database usernames.

4.02 Passwords

Procedure:

1. Each HMIS User will have a separate username and password for the HMIS database. This is not permitted to be shared or exchanged with any other users, unless authorized by the HMIS Administrator.
2. All Participating Agencies and Users shall keep both HMIS server and HMIS database passwords confidential, and protect the passwords by storing them in a safe place. They may not be shared with any other User, including other Users within the same agency.
3. Neither the HMIS Administrator nor designee will have access to passwords after passwords are initially created.
4. The HMIS Vendor will determine when and how often passwords will be reset.

4.03 Data Access Location

Procedure:

The HMIS Administrator will exercise the necessary precautions and care to protect Participant data confidentiality, follow all security policies in the HMIS Policies and Procedures Manual and adhere to the standards of ethical data use, regardless of the location of the connecting computer.

4.04 Data Requests

Procedure:

1. Requests for data shall be made to the HMIS Administrator in writing and will

include the date of the request, who is making the request, when the data is needed, the purpose for the request, and if applicable, a copy of the Participant Release.

2. Routine requests will be responded to in a reasonable time.
3. Emergency requests (e.g. discovery of error) will receive priority. Requestor should indicate preferred response time.

SECTION V
DATA ACCESS

Policy: Access to the database will be limited in order to protect the information within it and to protect the privacy of Participants. Access to HMIS Data shall be controlled with processes that ensure the confidentiality and security of the data and that allow for appropriate Participant access and access by other agencies and organizations to aggregate data.

5.01 Inter-Agency Data Sharing and Access Rights

Procedure:

1. Data included in the main profiles of the Participant (first entered when Participants are new) and Participant event (case) will be available in read-only access to all Users. The HMIS User(s) entering Participant profile information and establishing the case will have editing access to the data. Data change requests require HMIS Agency Administrator approval.
2. All Program and service level data can only be entered or amended by HMIS staff and/or the Participating Agency.

5.02 Access to Core Database

Procedure:

1. Only authorized HMIS Users and the Approved Software Vendor will have direct access to the HMIS database. No one will have direct access to the HMIS database through any means other than the Approved Software, unless explicitly given permission by the HMIS Administrator or designee during a process of software upgrade or conversion.
2. Use of HMIS data must be consistent with the Purpose Statement of this Policy as stated herein.

3. The Approved Software Vendor will provide access monitoring and will employ security methods to prevent unauthorized database access.

5.03 Data Retrieval

Procedure:

1. HMIS Users will maintain the security of any Participant data extracted from the database and stored locally as required by federal and state regulations, including all data used in custom reporting.

2. The HMIS Administrator or his/her designee may supply the Participating Agencies with specialized agency-level reports.

5.04 Participating Agencies

Procedure:

1. Participating Agencies will have access to retrieve any individual and aggregate data entered by their own programs.
2. Participating Agencies may view individual Participant's Case Notes entered by other Agencies only with the written consent of the Participant in question.

5.05 HMIS Software Vendor

Procedure:

1. The HMIS Software Vendor will not access individual or aggregate data contained within the HMIS, except in specific limited instances to correct system errors and/or inconsistencies. This excludes random viewing of records that may occur during troubleshooting or problem solving of software problems.
2. The HMIS Software Vendor or other software maintenance person will not require permission from the HMIS Committee to perform software maintenance, troubleshooting, and/or data conversion of the HMIS.

5.06 Participant

Procedure:

Participants who file a written, signed request to the HMIS Administrator to see their HMIS records will receive a printed copy of their records within five working days.

5.07 Public

Procedure:

Upon formal request, the HMIS Administrator will provide aggregate data information to appropriate agencies or bodies for acceptable use such as community planning, problem analysis, needs assessment, grant applications, and research.

SECTION VI
PARTICIPANT CONFIDENTIALITY

Policy: Confidentiality of Participant data (protected personal information, as defined in the HMIS Privacy Notice (see document E.4)), in compliance with all applicable federal and state confidentiality regulations, shall be of utmost importance to the HCCSC HMIS. Procedures shall be established and implemented to ensure that Participant information remains confidential in accordance with such laws and that Participants understand why their information is collected and how it is handled.

6.01 Ethical Data Use and Confidentiality

Procedure:

1. The HMIS Privacy Notice shall be provided to any individual upon request and may be posted on any website maintained by a Participating Agency. Each Participating Agency must post a sign stating the availability of the HMIS Privacy Notice to any individual who requests a copy.

2. The HCCSC and Participating Agencies shall comply with the following Confidentiality principles:

    a) Participant identifying information shall only be collected for the HMIS System for the purposes and in the manner described in the HMIS Privacy Notice.

b) Participant information, obtained in the course of professional service**,** should be protected unless there is a compelling reason to disclose it. Disclosure may be necessary to prevent serious, foreseeable, and imminent harm to a Participant or other identifiable persons.

c) Participants should be informed, to the extent possible, about disclosures and potential consequences. When feasible, the Participant should be informed prior to disclosure.

d) Participating Agencies should advise Participants and other interested parties about limits on Participants' right to confidentiality, such as the fact that publicly available information is not protected.

e) Participants will be informed about when confidential information may be legally required.

f) Confidentiality of Participants will be protected when responding to the media, and in written and electronic records or other communications.

g) Supplying identifying information should be avoided whenever possible.

3. A sign shall be posted at the intake desk(s) of walk-in locations and/or Participating Agencies explaining the reasons for asking for personal information which states that:

We collect personal information directly from you for reasons that are discussed in our privacy statement, which is available upon request. We may be required to collect some personal information by law or by organizations that give us money to operate this program. Other personal information that we collect is important to run our programs, to improveservices for homeless individuals, and to better understand the need of homeless individuals. We only collect information that we consider to be necessary and appropriate.

4. Ethical Use and Disclosure of Protected Information.

a) Participant identifying information shall only be used and disclosed for the purposes listed in the HMIS Privacy Notice and any other privacy notice of Participating Agency provided to a Participant.

b) Only information that is directly relevant to the purposes for which the disclosure is made should be revealed, and use of the information should be limited to the purposes for which it was revealed.

c) Each HMIS User will affirm the principles of ethical data use and Participant confidentiality contained herein by their signature on the HMIS User Agreements.

6.02 <u>Maintaining Participant Confidentiality</u>

E.1

Procedure:

All members of Stark County HMIS Lead Agency and Participating Agencies (including employees, volunteers, affiliates, contractors and associates) are required to sign a Stark County HMIS User Agreement that acknowledges receipt of a copy of the Privacy Notice and that pledges to comply with the Privacy Notice.

6.03 Participant Authorization and Rights

Procedure:

1. The Participant Informed Consent and Release of Information Authorization form (see document E.3) must be signed by each Participant seen in person whose data is to be entered into the HMIS. Verbal consent must be obtained in situations where the Participant is not seen in person, such as telephone intakes, registrations, and assessments. Participant refusal to sign the consent or verbally agree to data sharing will prevent individual data from being shared. The non-identifying data will still be used in aggregate reports.

2. Participating Agencies whose HMIS functions are covered by HIPAA entities must insert the date, event, or condition upon which the authorization will expire in order for the form to be HIPAA-compliant.
3. `42 CFR Part 2-covered Participating Agencies must insert the following in order for the form to be 42 CFR Part 2-compliant:
    a. The date, event, or condition upon which the authorization shall expire.
    b. Statement that "This information has been disclosed to you from records protected by federal confidentiality rules. 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 C.F.R. 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 information to criminally investigate or prosecute any alcohol or drug abuse participant."

4. Participants may revoke consent at any time through a written notice. Although the opt-out will stop the sharing of identifiable individual data, it will not cause data to be removed from the HMIS system.
5. No Participant may be denied services for withholding or revoking consent for identifying HMIS data collection. A standard participant revocation form will be available to all agencies.
6. Participants have a right to inspect, copy, and request changes in their HMIS records as outlined in the HMIS Privacy Notice.

7. HMIS Users will notify Participants that they can opt out of the HMIS database, except during the central intake process.
8. If a Participant opts out of HMIS but is served by HUD programs, data shall be entered under a special ID number and name to prevent Participant identification.

6.04 Participant Grievances

Procedure:

1. Resolution of Participant grievances shall be handled by the Agency alleged to have caused the grievance, pursuant to that Agency's grievance procedure.
2. Except for grievances that allege a violation of the HMIS User Agreement, Participating Agencies will not report HMIS-related Participant grievances to the HMIS Administrator.
3. All questions or complaints about Stark County HMIS privacy and security policies and practices will be accepted and considered.