1. Introduction

This manual contains the policies and procedures for the Chattanooga/Southeast Tennessee Continuum of Care (TN-500) Homeless Management Information System. All agencies and users who participate in this system are obligated to be familiar with and adhere to them.

1.1 HMIS Definition

Homeless Management Information System (HMIS) is a locally administered data system used to record and analyze client, service, and housing data for individuals and households who are experiencing homelessness or at risk of experiencing homelessness. The U.S. Department of Housing and Urban Development (HUD) and other planners and policymakers at the federal, state, and local levels use aggregate HMIS data to obtain better information about the extent and nature of homelessness over time. Specifically, an HMIS can be used to produce an unduplicated count of homeless persons, understand patterns of service use, and measure the effectiveness of homeless programs. Through HMIS, clients benefit from improved internal and external coordination that guides service and systems planning. Additionally, use of an HMIS helps avoid service duplication through the sharing of client data and project enrollments. A robust HMIS also helps communities engage in informed advocacy efforts, including the pursuit of policies that result in targeted services. Analysis of information gathered through HMIS is critical to accurately calculate the size, characteristics, and needs of different homeless subpopulations.

1.1.1 Source Documents

1. Homeless Management Information Systems (HMIS); Data and Technical Standards Final Notice, 2004
2. HMIS Requirements, Proposed Rule 24 CFR Part 580, 2011
3. 24 CFR Part 578, Continuum of Care Program Interim Rule, 2013
4. 24 CFR Parts 91 and 578, HEARTH: ESG Program Interim Rule, 2011

1.1.2 Historical Introduction

In 1999, Congress mandated the Department of Housing and Urban Development (HUD) to adequately track the scope of homelessness in the United States via the HUD Appropriations Act. In 2000 HUD mandated that each community implement or be in the process of implementation of a Homeless Management Information System (HMIS) by October 2004. HMIS is a secure

web-based centralized database where agencies providing services to those experiencing homelessness or housing instability share and report information about the clients that they serve.

1.1.3 HMIS Program Goals

1. **Measure the Extent and Nature of Homelessness:** This first goal is accomplished through analysis of homeless clients and service provider data. HMIS gathers an unduplicated count of those accessing services, service trends, bed utilization rates, re-entry rates, and HMIS system usage.
2. **Streamline the Intake and Referral Process for Human Service Agencies:** This second goal is achieved through the enforcement of a standardized mechanism for collecting client information across all providers. Standardizing intake procedures ensures all client information stored in HMIS is in a consistent and reliable format by project type.
3. **Improving Care Coordination Through Data Sharing:** This third goal is met in that HMIS provides a standardized mechanism for client information that can be shared among every participating human service agency to assist clients more efficiently and effectively. When a client shares information at an HMIS-participating agency, that information (except in certain circumstances) immediately becomes available to all other HMIS-participating agencies, meaning that clients do not have to repeat the same information time and time again to various providers.
4. **Assess Housing Inventory:** This fourth goal is fulfilled through the management of housing inventory assigned to each project within HMIS. Participating projects may, in real time, keep an updated list of occupied and available beds and units across various project types (emergency shelter, transitional housing, permanent supportive housing, etc.).

1.1.4 Annual Reports

Data collected and stored in HMIS is used in numerous federal, state, and local reports. Listed below are some common HMIS reports.

1. **The Longitudinal Systems Analysis (LSA)** - The LSA Report is an annual data submission that Continuums of Care (CoCs) provide to HUD. It uses HMIS data to track demographics, homelessness patterns, and housing outcomes over time. The report helps HUD assess system performance and informs national reports like the AHAR.
2. **The Housing Inventory Count (HIC)** - The HIC is an annual report submitted by CoCs to HUD that lists all beds and units available to serve people experiencing

homelessness, including the number of permanent housing beds. It includes details about project types, capacity, and funding sources, helping track resource availability in a community.

3. **The Point-in-Time Count (PIT)** - The PIT is a snapshot of homelessness taken on a single night each year by CoCs. It includes counts of both sheltered and unsheltered individuals and helps measure the scope of homelessness and inform local and national planning.
4. **System Performance Measures (SPMs)** - SPMs are annual metrics submitted by CoCs to HUD that evaluate how effectively a community is addressing homelessness. They track outcomes like length of time homeless, returns to homelessness, and housing placement rates.
5. **Annual Performance Reports (APRs)** - APRs are a required HUD report for CoC-funded projects that details program performance over the grant year. They include data on participant demographics, housing outcomes, and service delivery to assess project effectiveness.
6. **Consolidated Annual Performance and Evaluation Report (CAPER)** – The CAPER is an annual report submitted to HUD that outlines a jurisdiction's progress in meeting the goals and objectives of its Consolidated Plan. It details how CDBG, ESG, HOME, and other HUD funds were used, evaluates program outcomes, and demonstrates the impact of funded activities on low- and moderate-income communities.

1.2 HMIS Governance & Implementation

The governance of the HMIS shall fall to each of the parties outlined below, according to their stated responsibilities.

1.2.1 TN-500 Governance Council

The Governance Council (GC) shall be responsible for the following:

1. Designating a single HMIS and selecting the HMIS lead to make decisions about HMIS fees through the HMIS committee
2. Evaluating performance of the current HMIS lead agency

1.2.2 HMIS Lead Agency

The HMIS Lead Agency is the primary decision-making body for the TN-500 CoC HMIS, as designated by the TN-500 Governance Council and U.S Department of Housing and Urban Development (HUD). The responsibilities of the HMIS Lead Agency are as follows:

1. Operate a single HMIS.
2. Provide HMIS support to include training and data quality reviews for all HMIS participants.
3. Report HMIS aggregate data to the community, the state, and to federal partners (HUD, VA, HHS).
4. Apply for HMIS funds from HUD and other sources.
5. Make decisions about HMIS fees through the HMIS committee.
6. Monitor recipient and subrecipient participation in HMIS and report results to the HMIS committee.
7. Develop Data Quality, Security, and Privacy plans in consultation with the HMIS committee.
8. Identify service provider needs and challenges related to the HMIS.
9. Improve quality and completeness of service delivery system data.
10. Increase and monitor coordination of services.
11. Work with the GC HMIS Committee to develop strategies to encourage/recruit other agencies to participate in the HMIS.
12. Oversee HMIS operations and implement corrective actions to ensure compliance with federal requirements.
13. Contract with the designated HMIS vendor and ensure software compliance with HUD HMIS standards.
14. Implement HMIS policies and procedures to ensure high-quality data input from all participating agencies.
15. Execute written participation agreements with each agency, outlining roles, privacy and security obligations, sanctions, and data handling requirements.
16. Monitor and enforce agency compliance with HUD HMIS requirements and report to the CoC and HUD.
17. Ensure consistent HMIS participation by CoC, ESG, and partner programs such as FYSB RHY, HUD HOPWA, HHS PATH, and VA SSVF.
18. Extract and submit HMIS data in the required formats for HUD reports including APR, HIC, SPMs, and LSA.
19. Maintain an HMIS calendar of reports, monitoring, committee meetings, and trainings.

The HMIS Lead Agency for the TN-500 CoC is the Chattanooga Regional Homeless Coalition (CRHC), located at 5751 Uptain Rd., Ste 526, Chattanooga, TN 37411.

1.2.3 HMIS Committee

The goal of the HMIS Committee is to ensure the effective and efficient collection of data that is accurate and sufficient to monitor the homelessness response system and to

identify service gaps and other opportunities for system improvement. To achieve this goal, the HMIS Committee will:

1. Monitor performance of the CA's implementation and support of the HMIS.
2. Periodically update the GC on CA performance regarding HMIS implementation and support.
3. Work with the CA to identify service provider needs and challenges related to the HMIS.
4. Support the identification of service gaps by working with the CA to improve data quality, and to increase completeness of service delivery system data.
5. Help identify and implement ideas for leveraging HMIS capabilities to increase and monitor coordination of services.

1.2.4 Other Roles & Responsibilities

Other roles and responsibilities for various parties are outlined below.

1.2.4.1 HMIS Participating Agencies & End Users

1. Enter into a participation agreement before having access to HMIS.
2. Follow HMIS Policies and Procedures.
3. Comply with federal regulations regarding HMIS.
4. Comply with federal, state, and local laws that require additional privacy or confidentiality protection.
5. When privacy or security standard conflicts with other federal, state, and local laws to which the HMIS participating agencies must adhere, the agency must contact the HMIS Lead and collaboratively update the applicable policies for the agency to accurately reflect the additional protections.
6. Work with HMIS Lead on day-to-day operational issues.
7. Complete initial end-user training per prospective end-user prior to gaining system access.
8. Complete annual HMIS, Privacy, and Security Training
9. Designate a Data Champion

1.2.4.2 The Data Champion

The Data Champion acts as the primary point of contact between the HMIS Lead and the user agency for all data-related activities and initiatives, facilitating data quality improvement, overseeing training, and ensuring compliance with HMIS standards. Key responsibilities of the Data Champion include:

1. Overseeing and monitoring data quality for their agency
2. Receive and review Data Quality reports to identify areas needing improvement.
3. Facilitate data quality cleanup by coordinating with relevant staff and ensuring timely resolution of data issues.
4. Implement best practices and standard procedures for data entry to maintain high data quality standards.
5. Oversee training for agency/program staff on HMIS usage, data entry protocols, and data quality standards.
6. Ensure all staff members are adequately trained and updated on any changes in HMIS policies and procedures.
7. Provide ongoing support and guidance to staff to address any HMIS-related issues.
8. Serve as the liaison between the agency/program and the HMIS Team at the Chattanooga Regional Homeless Coalition
9. Communicate data quality issues, training needs, and system updates to agency/program team members
10. Participate in HMIS meetings, trainings, and workshops to stay informed about best practices and system updates.

2. Participating Agency Policies & Expectations

2.1 Adding a New Participating Agency

Prior to adding a new Participating Agency into HMIS, the HMIS Lead Agency will follow the procedures below:

1. Review records to ensure that the agency does not have previous HMIS policy violations.
2. Identify and verify the Data Champion for the agency.
3. Sign Participating Agency agreements.
4. Collect all required project data elements for the agency and project set up.
5. Ensure that the agency receives billing and pays the HMIS fees, if applicable.

2.2 Agreements

Participating Agencies are those agencies that use HMIS for the purposes of data entry, data editing, and data reporting. Relationships between the HMIS Lead Agency and Participating Agencies are governed by any standing agency-specific agreements and/or contracts already in place. The HMIS Lead Agency manages the HMIS Agency Participation

Agreement (Appendix A) and contents of the HMIS Policies and Procedures Manual. All Participating Agencies are required to abide by the policies and procedures outlined in this manual.

2.2.1 Partnership Termination-Data Transfer Policies

If the relationship between HMIS Lead Agency and a participating agency is terminated, the agency will no longer have access to the HMIS. The HMIS Lead Agency staff will make reasonable accommodations to assist the agency in exporting its data in a format that is usable in its alternative database. Any costs associated with exporting the data will be the sole responsibility of the participating agency.

2.3 Privacy Notice

HMIS participating agencies must post a sign stating the availability of its privacy notice to any individual who requests a copy. Participating agencies may either use the HMIS Privacy Notice (Appendix C) or their own privacy notice. If a participating agency chooses not to use the notice contained in this document, then it must include in the HMIS section of their notice at a minimum the same language found in the notice contained in this document.

2.3.1 Purpose Specification & Use Limitation

A participating agency must specify in its privacy notice the purposes for which it collects PII and must describe all uses and disclosures. They may use or disclose personally identifiable information (PII) only if the use or disclosure is allowed by this document and is described in its privacy notice. They may infer consent for all uses and disclosures specified in the notice and for uses and disclosures they determined to be compatible with those specified in the notice. Except for first party access to information and any required disclosures for oversight of compliance with HMIS privacy and security standards, all uses and disclosures are permissive and not mandatory. Uses and disclosures not specified in the privacy notice can be made only with the consent of the individual or when required by law.

2.4 Accountability

All participating agencies must establish an internal procedure for accepting and considering questions or complaints about their privacy and security policies and practices. They must require each HMIS end user (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.

2.5 Fee Schedule

HMIS participating agencies are expected to cover the fee per licensed end user as established by the HMIS Lead Agency in coordination with the HMIS Committee.

2.6 Training Schedule

All HMIS end users must complete training appropriate to their functions prior to gaining access to HMIS. A minimum of one training event is required per year for each licensed end user. Failure to complete these requirements will result in blocked access to HMIS. Additional training may be required if there are major system updates and/or regulatory changes. This additional training will be communicated as mandatory at the time the training is established. Additional training opportunities are outlined in the Data Quality Plan.

2.6.1 Annual Training

All HMIS users must attend annual training. The annual training will consist of a review of HMIS data elements, intake procedures, privacy and security standards, and any other items deemed important or necessary by the HMIS Lead Agency. Two training sessions will be offered each year, including an in-person option and a virtual option. All end-users must attend at least one of these meetings each year to maintain HMIS access.

2.6.1.1 Training for Victim Service Providers

Victim Service Providers (VSP) will be invited to attend HMIS training opportunities given the overlap in required data elements for VSP projects; however, attendance will not be made mandatory.

2.6.2 Training Record Keeping

HMIS Lead Agency staff will maintain records of those in attendance at each annual meeting in order to ensure that all licensed end users have complete training requirements.

3. End User Administration

3.1 New User Prerequisites

All user candidates are required to have basic computer skills as a prerequisite to receiving HMIS access. Prior to scheduling HMIS training, participating agencies should confirm that user candidates have basic computer skills. Prior to requesting training, participating

agencies will require all candidates' users to obtain any skills they lack from the list of computer competencies below.

1. Hardware: Users must be familiar with locking workstations, updating operating systems, and keyboard shortcuts.
2. Internet Browser Security: Users must be able to clear the internet browser cache and be familiar with privacy settings and password protocols.
3. Software: Users must be familiar with collapsing/expanding navigation menus, file naming and file types, digital form functionality, etc.
4. Privacy: Users must be able to capture and remove personally identifiable information (PII) from screenshots and understand the use of encryption to send sensitive data.

3.2 New User Security and Screening

All HMIS participating agencies are responsible for conducting criminal background checks on prospective end users prior to requesting HMIS access. This process must include a review for any history of fraud or other relevant criminal activity that could impact the integrity or appropriate use of the HMIS. If the agency uncovers any information that may fall into these categories, it is responsible for notifying the HMIS Lead Agency. Prospective users with a criminal history that may impact the integrity or appropriate use of the HMIS may be denied access by the HMIS Lead Agency. The HMIS Lead Agency staff reserves the right to review end users' criminal history checks.

3.3 New User Requirements

To be issued a license, prospective users must complete the initial end user training, including agreeing to and signing the HMIS End User Agreement (Appendix B). At that time, they will also be required to read and acknowledge receipt of these policies and procedures. New user training will be arranged as soon as the candidate user has met all the preceding requirements listed above and the agency requests training. Training is conducted on an individual basis and is self-paced. See Data Quality Plan for more details.

3.4 User Permissions

The HMIS Lead Agency staff will assign to each user only the access level required to perform the user's assigned duties, as agreed upon with the participating agency. This assignment will be the lowest access level needed for the user to perform their work, as defined by their position and duties at the agency. If the user's responsibilities or position changes, HMIS should be contacted to determine if a change in access level is required. Only HMIS staff may perform the issuance, modification, and revocation of user licenses. The

participating agency is responsible for notifying the HMIS staff of potential new users, as well as any changes to existing user roles which require license modification or cancellation.

4. Data Disclosures and Sharing Limitations

4.1 Data Collection

Participating agencies are expected to maintain current knowledge of and adhere to the data collection requirements identified by the federal partner(s) funding their projects. Each of the federal partner programs using HMIS has a specific manual describing the project set up in HMIS and what data elements are required to be collected. Participating agencies must review their most current program HMIS manuals to ensure that all required program-specific data elements (PSDEs) designated by their funding stream(s) are being collected. Agencies should consult relevant federal manuals as needed.

4.2 Collection Limitations

A participating agency may collect PII only when appropriate to the purposes for which the information is obtained or when required by law. A participating agency must collect PII by lawful and fair means and with the knowledge or consent of the individual. The consent of the individual for data collection may be inferred from the circumstances of the collection.

When collecting PII during application, intake, and case management, the clients must understand why this data is being collected. A sign must be posted at each intake desk (or comparable location) or a verbal description given that explains generally the reasons for collecting this information. The reason for collecting any information during the HMIS intake process that does not directly relate to the specific services requested by the client should be briefly explained by the intake staff during the intake process.

4.2.1 Collection Guidelines

The following guidelines should be adhered to when collecting information from a client:

1. PII collected by a participating agency must be relevant to the purpose for which it is to be used. To the extent necessary for those purposes, PII should be accurate, complete and timely.
2. Clients have the right to refuse to provide the answer to any required data elements. Their refusal might have an impact on project eligibility; however, their refusal is an acceptable answer in regard to HMIS. Motivational interviewing techniques are encouraged to ensure that clients rarely refuse or simply state that they don’t know the answer.

3. Client consent is not required to enter information into the HMIS; consent is only required to share that information with other participating agencies. However, due to system limitations, client profiles entered into the HMIS are automatically visible to all participating agencies. As a result, agencies must obtain client consent before entering any information they do not wish to be shared. Accurate data entry remains essential for reporting to funding agencies.
4. Client aliases are permissible and expected in the cases of any information related to those fleeing domestic violence or who are actively being engaged by outreach workers. Outside of these groups, collecting incomplete data or using aliases is generally discouraged, as this practice negatively impacts overall data quality and care coordination within the system.

4.3 Data Sharing

TN-500 requires clients to consent to share their data. Most housing service providers have visibility to all client data for which consent has been given. However, agencies that provide services beyond the scope of housing and homelessness may also be granted HMIS access. In these instances, such organizations may have different sharing parameters as determined by the HMIS administrator.

4.4 Disclosures

Each of the participating agencies must comply with the following uses and disclosures, as outlined in the HUD Data Technical Standards: Final Notice. A participating agency has the right to establish additional uses and disclosures as long as they do not conflict with these uses and disclosures.

A participating agency may use or disclose PII from HMIS under the following circumstances:

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; or
4. For creating de-identified PII (“Anonymous”).
5. A participating agency may use or disclose PII when required by law to the extent that the use or disclosure complies with and is limited to the requirements of the law.

6. Use and disclosures avert a serious threat to health or safety. A participating agency may, consistent with applicable law and standards of ethical conduct, use or disclose PII if:
7. The participating agency, in good faith, believes the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public; and
8. The use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat.

A participating agency may disclose PII about an individual whom the agency reasonably believes to be a victim of abuse, neglect or domestic violence to a government authority (including a social service or protective services agency) authorized by law to receive reports of abuse, neglect or domestic violence under any of the following circumstances:

1. Where the disclosure is required by law and the disclosure complies with and is limited to the requirements of the law.
2. If the individual agrees to the disclosure; or
3. To the extent that the disclosure is expressly authorized by statute or regulation; and the participating agency believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or if the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the PII for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

A participating agency that makes a permitted disclosure about victims of abuse, neglect or domestic violence must promptly inform the individual that a disclosure has been or will be made, except if:

1. Where the disclosure is required by law and the disclosure complies with and is limited to the requirements of the law.
2. If the individual agrees to the disclosure; or
3. To the extent that the disclosure is expressly authorized by statute or regulation; and the participating agency believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or if the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the PII for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.

A participating agency that makes a permitted disclosure about victims of abuse, neglect or domestic violence must promptly inform the individual that a disclosure has been or will be made, except if:

1. The agency, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or
2. The agency would be informing a personal representative (such as a family member or friend), and the agency reasonably believes the personal representative is responsible for the abuse, neglect or other injury, and that informing the personal representative would not be in the best interests of the individual as determined by the agency, in the exercise of professional judgment.

A participating agency may use or disclose PII for academic research conducted by an individual or institution that has a formal relationship with the agency if the research is conducted either:

1. By an individual employed by or affiliated with the organization for use in a research project conducted under a written research agreement approved in writing by a program administrator (other than the individual conducting the research) designated by the agency; or
2. By an institution for use in a research project conducted under a written research agreement approved in writing by a program administrator designated by the agency.
3. A written research agreement must:
    a. Establish rules and limitations for the processing, anonymizing, and security of PII in the course of the research.
    b. provide for the return or proper disposal of all PII at the conclusion of the research;
    c. restrict additional use or disclosure of PII, except where required by law; and
    d. require that the recipient of the data formally agrees to comply with all terms and conditions of the agreement.
4. A written research agreement is not a substitute for approval of a research project by an Institutional Review Board, Privacy Board or other applicable human subjects' protection institution.

The following policy has been established for handling inquiries from law enforcement personnel (whether local, state, or federal) regarding HMIS data:

1. Require Written Requests
    a. Law enforcement personnel seeking any data in HMIS should submit a formal, written request explaining what information they are seeking and the reason why they are seeking it.
2. Escalation to HMIS Lead:

    a. Any requests from law enforcement personnel (including local, state, and federal officers and agents) for HMIS data, whether directed to a TN-500 HMIS Participating Agency, or any other entity, must be escalated immediately to the designated HMIS Lead.
    b. No further action should be taken by the agency or entity that received the request until instructed by the HMIS Lead.
3. Role of the HMIS Lead and Legal Counsel:
    a. The HMIS Lead will consult with legal counsel to ensure that any response to such inquiries complies with applicable laws and regulations.
    b. Agencies collecting and entering data into HMIS must refrain from sharing any HMIS data directly with law enforcement unless explicitly directed by the HMIS Lead after consultation with legal counsel.
4. Compliance with Legal Disclosures
    a. Disclosures mandated by law, including those pursuant to court orders, are permissible to the extent that they comply with and are limited to the specific requirements of the law.
    b. Such disclosures must adhere to the 2004 Data and Technical Standards Final Notice and any subsequent HUD guidance.
    c. Any information disclosures mandated by law and authorized by the HMIS Lead will be limited to the minimum amount of data necessary to comply with the legal request.
5. Documentation:
    a. The HMIS Lead will document all law enforcement requests and responses, ensuring transparency and compliance with legal standards.
6. Privacy Policy and Law Enforcement Requests
    a. Designated Point of Contact: The HMIS Lead is the sole entity authorized to respond to law enforcement requests for data from HMIS or a comparable database.
    b. Responsibility of the HMIS Lead: It is the responsibility of the HMIS Lead to consult with legal counsel regarding the appropriate response to such requests.
    c. Participant Privacy Protections: The Privacy Policy emphasizes the protection of participant privacy and ensures that no data is disclosed without adherence to proper legal protocols.

4.5 Data Expiration

A participating agency must develop and implement a plan to dispose of or, in the alternative, to remove identifiers from PII that are not in current use seven years after the PII was created or last changed (unless a statutory, regulatory, contractual, or other requirement mandates longer retention). Unless required for longer retention after 7 years from the last service, paper records of PII must be disposed of properly by law and in such a manner that the information is unrecoverable. Alternatively, the paper copies can be retained; however, the PII must be removed such as blacking out the data. Electronic PII must also be purged after 7 years.

4.6 Previous Clients as End Users

Any prospective end user who has resided at or participated in a housing program in the TN-500 Continuum of Care and intends to work or volunteer for an HMIS participating agency in a capacity requiring their use of HMIS, must have exited the project no less than 12 months prior to HMIS licensing.

4.7 Members of Law Enforcement as End Users

No active member of law enforcement, detention, and/or corrections staff shall be a licensed HMIS user. To protect the privacy and confidentiality of CoC Clients, active members of law enforcement will not be granted access to HMIS. Limited exceptions may be negotiated, in cases of a Partner Agency project serving clients currently incarcerated or facing detention who are also at risk of or experiencing homelessness, such as jail diversion or prison release projects. Retired law enforcement professionals who become volunteers or employed staff members at a Partner Agency post-law enforcement career may become users of HMIS when it is imperative to their responsibilities.

4.8 Protection for Domestic Violence

Any VSP serving victims of domestic violence, dating violence, sexual assault or stalking; funded by the Family Violence Prevention and Services Act, Office for Victims of Crime, or Office on Violence Against Women; or receiving Specialized Housing and Services for Victims of Human Trafficking funds are not allowed to participate in HMIS; however, may be required by a funding agency to maintain the same universal data elements on a comparable database system. As such, the guidelines established by this manual should be considered minimal requirements.

5. Violation of Policies

If a participating agency or any of its users may have violated any HMIS policy, the HMIS lead will implement an action plan upon discovery of the violation. Policy violations including but not limited to security breaches, then HMIS lead will implement an action plan that will include the following stages of response:

1. **Probation**: The HMIS Lead Agency staff will notify the participating agency's point of contact in writing to set up a one-on-one meeting to discuss the violation in question. During the meeting, an action plan will be developed and documented with relevant time frames outlined to correct actions. If a training issue is identified, HMIS Lead Agency staff will coordinate further follow-up with the users in question. The participating agency will be placed on probation, for a minimum of 90 days, where monitoring and auditing may be required and performed regularly during this period.
2. **Suspension**: If a violation is of critical risk or the corrective measure(s) are not achieved in the probationary period, or more HMIS violations occur during the probationary period, the HMIS Lead Agency staff will suspend access to HMIS until the issues are resolved The participating agency's CEO or Executive Director will receive a written notice of the suspension, reasons, and effective date. During suspension, a mandatory meeting will be held between the participating agency's CEO or Executive Director, and the HMIS administrator, if appropriate, to discuss suspension and requirements for resolution. All meeting deliverables will be documented in writing and must be achieved within the set probationary period.
3. **Termination**: Agencies with projects required to participate in HMIS: If the participating agency violates any policies deemed of critical risk and fails to achieve resolution within the probation period, the HMIS Administration after consultation with the participating CEO or Executive Director will determine a course of action to resolve the issue. Depending on the violations, the participating agency may be allowed read only access or complete removal from HMIS while data is entered by the HMIS lead staff at a cost to the agency. The participating agency's CEO or Executive Director will receive a written notice outlining the determination, reasons, effective date, and associated costs. This determination will also be reported to the participating agency's funder and in the case of the CoC Program projects, the program review committee/ranking committee.
4. **Agencies not required to participate in HMIS**: If the participating agency violates any policies deemed of critical risk and fails to achieve resolution within the probation period, the HMIS Administration will permanently terminate the participating agency from HMIS. The participating agency will receive a written

notice to the participating agency's CEO or Executive Director outlining the termination, reasons, and effective date.

6. Client Rights

Clients participating in or receiving services from participating service providers have the right to privacy and confidentiality as well as a complete understanding of how their data can or will be used with HMIS. Clients should be informed of the following statements prior to enrolling in HMIS:

1. Clients have a right not to answer any questions, even if they are required for enrollment into a program; however, failure to answer questions required for entry may result in the client not being admitted into a program.
2. Client information may not be shared without informed consent.
3. Every client has a right to an understandable explanation of HMIS and what "consent to participate" means. The explanation shall include:
    a. Type of information collected
    b. How the information will be used
    c. That refusal to provide consent to collect information shall not be grounds for refusing entry into the program.

6.1 Participation Opt Out

All clients enrolling in a CoC funded project will have data entered into HMIS. Client may prohibit the sharing of data specific to their enrollment (including case notes, services, etc. But not PII). Services cannot be refused if the client chooses to opt out of sharing data in HMIS. However, clients may be refused program entry for not meeting other agency eligibility criteria. If a client previously gave consent to share information in HMIS and chooses at a later date to withdraw consent, the client must inform the enrolling agency in writing to update data sharing preferences.

6.2 Access to Records

A client has the right to request access to their personal information stored in HMIS from authorized agency personnel. The agency, as the custodian of the client data, has the responsibility of providing the client with the requested information, in a timely manner except were exempted by state and federal law. When requested, a client may view his or her own data or the data of a dependent, contained in HMIS. No client shall have access to another client's records within HMIS.

Agency staff must respond to client requests for access to their HMIS data within 30 calendar days of receipt of the request. This time frame ensures that data is shared in a manner

that upholds the principles of data security and information privacy. All responses must follow established procedures for secure transmission of sensitive information.

Clients have the right to request that their HMIS data be amended if they believe the information is inaccurate or incomplete. Agency staff must review and respond to such requests within 30 calendar days of receipt. All amendment requests must be documented. If a request is denied, the agency must provide a written explanation outlining the reason for the denial, and this explanation must also be documented in the client's record.

In the privacy and security training, agency staff will be trained to respond in a trauma-informed manner regarding client requests for their own data.

7. Security

7.1 Technology Requirements

The HMIS lead agency is responsible for each participating agency's oversight and adherence to the current HUD HMIS Data and Technical Standards. All agencies will be subject to periodic on-site security assessments to validate compliance of the agency's security protocols and technical standards.

7.2 Hardcopy Security

A participating agency must secure any paper or other hard copy containing PII that is either generated by or for HMIS, including, but not limited to reports, data entry forms, priority lists, and signed consent forms. A participating agency must maintain control of any paper or other materials containing PII generated for or by HMIS at all times when such materials are in a public area. When staff are not present, the information must be secured in areas that are not publicly accessible. Hard copies of data stored or intended to be stored in HMIS, regardless of whether the data has yet been entered into HMIS, will be treated in the following manner:

1. Records shall be kept in individual locked files or in rooms that are locked when not in use.
2. When in use, records shall be maintained in such a manner as to prevent exposure of PII to anyone other than the user directly using the record.
3. Employees shall not remove records or other information from their places of business without permission from appropriate supervisory staff unless the employee is performing a function which requires the use of such records outside of the participating agency's place of business and where return of the records by the close of business of would result in the undue burden on staff.

4. When staff remove records from their places of business, the records shall be maintained in a secure location and staff must not disclose the PII contained in those records except as permitted by these policies and procedures.
5. Faxes or other printed documents containing PII shall not be left unattended.
6. Fax machines and printers shall be kept in secure areas.
7. When faxing PII, the recipients should be called in advance to ensure the fax is properly managed upon receipt.
8. When faxing, copying or printing, all documents containing PII should be removed from the machines promptly.
9. HMIS information in hardcopy format should be disposed of properly to ensure information is unrecoverable.

8.3 Electronic Storage, Transfer, & Disposal

Participating agencies and users are responsible for maintaining the security and confidentiality of any client-level data extracted from the database and stored locally, including all data used in internal reporting. At a minimum, the following best practices must be applied to all HMIS data:

1. All data downloaded on to a data storage medium must be maintained and stored in a secure location.
2. The data storage medium must be password protected.
3. Any data downloaded onto a data storage medium must be disposed of by reformatting as opposed to being erased or deleted.
4. Data storage medium must be reformatted a second time before the medium is reused or disposed of.
5. Data downloaded for the purposes of statistical analysis must exclude PII whenever possible.
6. PII data is not to be electronically transmitted (including email, attachments, reports, screenshots, text messages, etc.) unless it is properly protected.

8.4 HMIS Disaster Recovery

The HMIS database must have backup systems that allow the data to be recovered in the event of a disaster. The HMIS vendor is expected to have database backups in at least one city distant from the main database housing.

In accordance with standards, the HMIS Vendor software hosting and back up data center should be a SSAE 16 certified data center. Incremental database backups are performed every 4 hours and full database backups are performed each day and sent offsite weekly to a

second geographically dispersed SSAE 16 storage facility. The following recovery process should include:

a) Restoration procedures for the application and data at the host level.
b) Recovery procedures for historical data at the host level.
c) A stated recovery time after a planned or unplanned outage, power interruption, or system crash.

8.5 Data Security Incidents

All HMIS users and their agencies are obligated to report suspected instances of noncompliance with policies and procedures that may lead to a security breach of HMIS data.

1. **Violations of Hardcopy Security**: Any user or agency that has a violation of hardcopy security is expected to investigate this internally by reviewing their privacy and security policies and procedures to ensure that they are appropriate and include at a minimum those policies and procedures outlined in this HMIS policies and procedures. They should also then evaluate if they have a training issue regarding their policies and procedures. Finally, they should act on the violation according to their policies and procedures.
2. **Violations of HMIS Database Security**: If the HMIS might have been compromised, then the HMIS Administrator is to be notified as soon as possible to take appropriate actions on user accounts and conduct an audit on potential data breach. As well as reporting incidents to appropriate legal authorities. In cases of a confirmed systemic breech participants will be notified by HMIS administration.

In instances of serious data security violations, the HMIS Lead Agency shall provide a mechanism—such as an anonymous reporting form—to allow HMIS participating staff to confidentially report observed or suspected violations.

8. Data Quality

HMIS participating agencies and end users are responsible for ensuring HMIS data quality. Data quality refers to the timeliness, accuracy and completeness of information collected and reported in HMIS. Adherence to set data quality standards will help bring additional funding into our community as well as ensure our community's level of service is accurately reported locally, statewide, and nationally. Data quality will be evaluated on completeness, consistency, accuracy, and timeliness. This data will be used by the CoC to monitor progress towards meeting its standards. Partner Agencies should review the Data Quality Plan to ensure they are maintaining quality data best practices.

9. Monitoring Policies

HMIS participating agencies and the HMIS Lead Agency will be monitored regularly to ensure that all HMIS policies and procedures are being followed as well as provide key data to enhance system performance.

9.1 HMIS Participating Agency Monitoring

Participating agencies will be monitored by HMIS Lead Agency throughout the year. The monitoring is to ensure that agencies remain in compliance with these HMIS policies and procedures. The HMIS Participating Agency Monitoring Checklist (Appendix D) will be used during the on-site monitoring. The monitoring site visit will be scheduled in advance, and the point of contact will receive a copy of the checklist prior to the scheduled visit.

9.1.1 Privacy Monitoring

At the time of the agency monitoring, participating agencies will also be monitored annually to ensure that the privacy policies and procedures are followed using the monitoring checklist.

9.1.2 Security Monitoring

Participating agencies will be monitored annually by the HMIS lead agency. HMIS staff will schedule and visit the participating agency on site to ensure that the hard copy and technical safeguard policies and procedures are being followed using the monitoring checklist.

9.2 HMIS Lead Annual Monitoring

Annually, the HMIS Lead/Management will be monitored by the TN-500 Governance Council to ensure that its oversight of the HMIS meets the CoC's expectations.

10. Supplementary Documents

In addition to these policies and procedures, the following documents will serve to provide additional guidance regarding data quality, privacy, and security.

1. The Data Quality Plan (DQP) - The Data Quality Plan serves to
2. The Privacy and Security Plan (PSP) - The Privacy and Security Plan serves to

11. Terminology

1. **Continuum of Care and Continuum (CoC)** - the group organized to carry out the responsibilities required under the CoC Program Interim Rule (24 CFR Part 578) and is comprised of representatives of organizations, including nonprofits, victim service providers, faith-based organizations, governments, businesses, advocates, public housing agencies, school districts, social service providers, mental health agencies, hospitals, universities, affordable housing developers, law enforcement, and organizations that serve people experiencing homelessness or housing instability or who have previously experienced homelessness or housing instability to the extent that these groups are represented within the geographic area and are available to participate.
2. **Homeless Management Information System (HMIS)** - A Homeless Management Information System is a local information technology system used to collect client-level data and data on the provision of housing and services to individuals and families at-risk of and experiencing homelessness in the CoC service area.
3. **Coordinated Entry (CE)** - a centralized or coordinated process designed to coordinate program client intake, assessment, and provision of referrals across CoC service area. The CE is easily accessed by individuals and families seeking housing or services, is well advertised, and includes a comprehensive and standardized assessment tool.
4. **By-Name-List (BNL)** - a holding list that all agencies use that contains the names of individuals or families that have been identified and assessed and need some type of housing intervention. This list assists in determining the clients that have met eligibility requirements and are awaiting housing placement.
5. **Participating Agency** - An agency, organization, or group that has signed an HMIS Participating Agency Agreement for the purpose of utilizing HMIS within the TN-500 Continuum of Care.
6. **Program-Specific Data Elements (PSDEs)** - Program-Specific Data Elements provide information about the characteristics of clients, the services that are provided, and client outcomes. The HMIS Federal Partners have cooperatively developed these elements. Some of the program specific data elements are collected across all federal partner programs. Others are limited to a single federal partner program or even further to a single component of one of the federal partner programs.
7. **Personally Identifiable Information (PII)** - Defined in OMB M-07-16 as "...information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

8. **HMIS Lead Agency** - entity designated by the Continuum of Care in accordance with the HMIS Proposed Rule (24 CFR Part 580) to operate the Continuum's HMIS on the Continuum's behalf.
9. **Client** - refers to an individual or household who: is currently experiencing homelessness, at risk of homelessness or in recovery from homelessness.

12. Appendix A - HMIS Participating Agency Agreement

MEMORANDUM OF AGREEMENT
between
TN-500 Homeless Management Information System Lead Agency
and
{Participating Agency}

I. Introduction: Homeless Management Information System (HMIS) is a locally-administered data system used to record and analyze client, service, and housing data for individuals and families who are experiencing homelessness or at risk of experiencing homelessness. The U.S. Department of Housing and Urban Development (HUD) and other planners and policymakers at the federal, state, and local levels use aggregate HMIS data to obtain better information about the extent and nature of homelessness over time. Specifically, an HMIS can be used to produce an unduplicated count of persons experiencing homelessness, understand patterns of service use, and measure the effectiveness of homeless programs. Through the HMIS, clients benefit from improved internal and external coordination that guides service and systems planning. Additionally, use of the HMIS helps avoid service duplication through the sharing of client data and project enrollments. A robust HMIS also helps communities engage in informed advocacy efforts, including the pursuit of policies that result in targeted services. Analysis of information gathered through HMIS is critical to accurately calculate the size, characteristics, and needs of different homeless subpopulations.

II. TN-500 HMIS Lead Agency will:

1. Oversee and coordinate all aspects of the HMIS implementation and development.
2. Serve as the sole contact with the HMIS software vendor and monitor its performance under its contract.
3. Oversee system administration especially as it relates to privacy and security protocols.
4. Notify the Participating Agency of HMIS software failure, errors, and/or problems immediately upon discovery.
5. Provide help desk service during designated open hours.
6. Monitor privacy, confidentiality, and security protocols for the HMIS.
7. Monitor the data quality of the HMIS.
8. Oversee and coordinate the HMIS activities of the agency HMIS point of contact (POC).
9. Provide ongoing training on the use of the HMIS software.
10. Provide support to and function as a resource to the users and the agency administrator, if applicable; and

11. Provide reports requested by the Participating Agency within a reasonable time.

III. Participating Agency will appoint at least one person to serve as the HMIS Data Champion for the agency, and this person will:

1. Overseeing and monitoring data quality for their agency
2. Receive and review Data Quality reports to identify areas needing improvement.
3. Facilitate data quality cleanup by coordinating with relevant staff and ensuring timely resolution of data issues.
4. Implement best practices and standard procedures for data entry to maintain high data quality standards.
5. Oversee training for agency/program staff on HMIS usage, data entry protocols, and data quality standards.
6. Ensure all staff members are adequately trained and updated on any changes in HMIS policies and procedures.
7. Provide ongoing support and guidance to staff to address any HMIS-related issues.
8. Serve as the liaison between the agency/program and the HMIS Team at the Chattanooga Regional Homeless Coalition
9. Communicate data quality issues, training needs, and system updates to agency/program team members
10. Participate in HMIS meetings, trainings, and workshops to stay informed about best practices and system updates.

IV. Agency Obligations: The HMIS Participating Agency agrees to maintain the confidentiality of all client information disclosed or entered into the HMIS in accordance with the TN-500 HMIS Policies & Procedures. Moreover, the HMIS Participating Agency agrees to abide by the data quality, security, and privacy standards outlined TN-500 HMIS Policies & Procedures, the Data Quality Plan, and the Privacy and Security Plan.

V. License Cost and Termination: The HMIS Lead Agency in consultation with the HMIS Committee determines the cost of HMIS participation

VI. Term of Agreement:

1. Term: This Agency Participation Agreement (APA) is effective on date it is countersigned by the CEO or Executive Director on the signature page of this Agreement and shall remain in effect for 1 year (“Initial Term”) unless terminated pursuant to paragraph VI 2 hereof. This APA shall automatically renew each year on

the anniversary date, subject to termination as provided in paragraph VI 2 hereof. If the Participating Agency chooses not to renew this Agreement, the CEO or Executive Director shall notify the HMIS Lead Agency Executive Director of nonrenewal at least 30 days before the expiration of the then-current term.

2. Termination: Either party has the right to terminate this APA with a 30-day prior written notice to the other party. The HMIS Lead Agency reserves the right to amend the APA with a 30-day notice sent to all Participating Agencies.

3. If either party believes the other to be in default of any one or more of the terms of this APA, that party will notify the other in writing of such default; and
4. The other party shall then have ten business days in which to cure such default.
5. If such default is cured within such period, this APA will continue in effect.
6. If such default is not cured within such period, the non-defaulting party shall have the right to declare the APA to be immediately terminated.
7. If this APA is terminated, the HMIS Lead Agency and its remaining participating agencies shall retain their right to the use of all client data previously entered by the terminating Participating Agency, subject to any restrictions requested by the client. The HMIS management staff will make reasonable accommodations to assist the Participating Agency to export its data in a format that is usable in its alternative database. Any costs associated with exporting the data will be the sole responsibility of the participating agency.

VII. Agreement: By signing below, I agree to the stipulations of this Agreement and agree that my agency will abide by the TN-500 HMIS Policies and Procedures Manual.

TN-500 HMIS Lead Agency Executive Director

Signature: _____ Date: _____

CEO or Executive Director or Designee of {participating agency}

Signature: _____ Date: _____

Name of Agency: _____

Name of Agency Data Champion: _____

13. Appendix B - HMIS End User Agreement

The following language is taken from the end of the initial HMIS end user training. All new trainees are expected to agree to the following to be granted access to the HMIS.

TN-500 Homeless Management Information System (HMIS) End User Agreement

Homeless Management Information System (HMIS) is a locally administered data system used to record and analyze client, service, and housing data for individuals and families who are experiencing homelessness or at risk of experiencing homelessness. This data demonstrates the extent and nature of homelessness over time, produces an unduplicated count of people experiencing, and assists the TN-500 Continuum of Care to measure the effectiveness of homeless assistance projects and programs. Data produced is used for planning, education, and submission of reports to the Department of Housing and Urban Development (HUD) and other federal partners.

Prior to granting you access to HMIS, you must sign this user agreement acknowledging the key requirements for accessing the system and the core tenets of client confidentiality and rights. You can learn more about the items below in the HMIS Policies and Procedures Manual. Also, your new user training will cover them in more detail. There is also an expectation that you will read the HMIS Policies and Procedures Manual prior to CoC's annual HMIS training that is required of all users.

By signing this, you agree to the following:

1. I meet all user prerequisites stated in the HMIS Policies and Procedures Manual.
2. My HMIS user ID and password are for my use only and must not be shared with anyone or stored on any computer for automatic login.
3. HMIS must only be accessed through secure computers/internet in compliance with the HMIS Policies and Procedures Manual.
4. I must log off the HMIS software before leaving the area where the workstation is located.
5. All HMIS information (hard copies and soft copies) must be kept secure and confidential at all times.
6. When no longer needed, any documents or data containing HMIS information must be properly destroyed.
7. I understand that if I notice or suspect a security breach within the HMIS, I must immediately notify my agency HMIS Data Champion and the HMIS Lead Agency Staff.
8. HMIS users may not share client data with individuals or agencies that have not entered into an HMIS participation agreement or without obtaining written

permission from the client.

9. Information in the HMIS may not be accessed beyond what is required for job performance.
10. No client may be denied services for failure to provide consent for HMIS data collection.
11. Client consent must always be obtained before data is entered into HMIS, whether verbally or written.
12. Clients have a right to inspect, copy, and request changes to their HMIS records.
13. Client consent may be revoked by the client at any time through a written request.
14. Any HMIS user found to be in violation of the HMIS Policies and Procedures, or the points of client confidentiality in this user agreement, may be denied access to the HMIS.

14. Appendix C - Privacy Notice

TN-500 HMIS Privacy Notice

This notice describes how personal information is collected, used, and protected within the TN-500 Homeless Management Information System (HMIS). By requesting services, you are presumed to consent to the collection and use of your information as outlined below and as required by law.

Why We Collect Information

We collect personal information to improve services, coordinate care, meet funder requirements, and better understand homelessness in our community. This may include your name, date of birth, Social Security number, housing history, and services received. Your data is stored securely and shared only with other authorized HMIS participating agencies for service coordination and reporting purposes.

How Your Information May Be Used or Shared

We do not share your personal information without your consent unless legally required or permitted as listed below. Your information may be used or shared:

1. To provide or coordinate services
2. For payment, program operations, or audits
3. When required by law
4. To prevent harm or respond to abuse, neglect, or violence
5. For approved research or law enforcement under specific legal conditions

Your Rights

You may request to view or correct your personal information at any time. Requests may be denied under specific circumstances, such as risks to safety or confidentiality. You will be informed of the reason if your request is denied. You may also request to cease sharing information at any time.

Questions or Complaints

If you have concerns about your privacy or believe your information has been misused, contact the Chattanooga Regional Homeless Coalition at (423) 710-1501. All HMIS users are required to comply with this privacy notice.

15. Appendix D - HMIS Participating Agency Monitoring Checklist

The annual monitoring conducted by the HMIS Lead Agency for HMIS Participating Agencies will, at a minimum, cover the following topics.

1. The HMIS Participating Agency has a copy (physical or virtual) of the latest HMIS Policies and Procedures manual.
2. The HMIS Participating Agency has a signed APA on file (physical or virtual).
3. All active end users have completed (or have registered for) initial end user and annual required training.
4. All HMIS fees owed under the applicable schedule have been paid in full and are current as of the date of the APA.
5. Quality, accuracy, completeness, and timeliness of data entry into HMIS by project type.
6. Accessibility protocols for non-native English speakers or individuals with visual or hearing impairments.
7. The HMIS Participating Agency has a visible privacy notice posted in a common area.
8. The HMIS Participating Agency meets or exceeds standards of Data Quality as set forth in the DQP.
9. The HMIS Participating Agency meets or exceeds standards of Privacy and Security as set forth in the PSP.