Nashville-Davidson County
HMIS Policies and Procedures Manual

Metro Homeless Impact Division

Contents

Section 1: Introduction 3
Section 2: HMIS Lead Agency Roles & Responsibilities 3
Section 3: HMIS Member Agency Roles & Responsibilities 4
Section 4: User Administration 8
Section 5: Clients' Rights 10
Section 6: Privacy, Safety & Security 13
Section 7: User Training 16
Section 8: HMIS Technical Support 17
Section 9: Data Collection 17
Section 10: Data Quality 19
Section 11: Performance Measurement 20

Section 1: Introduction

The McKinney-Vento Homeless Assistance Act, as amended by the Homeless Emergency Assistance and Rapid Transition to Housing (HEARTH) Act of 2009, codified the congressional mandate for the U.S. Department of Housing and Urban Development (HUD) to report annually on homelessness at the national level. The Act requires that Continuums of Care (CoC) use a community-wide homeless management information system (HMIS) to:

1. Collect unduplicated counts of individuals and families experiencing homelessness;
2. Analyze patterns of use of assistance provided to persons experiencing homelessness; and
3. Provide information to project sponsors and applicants for needs analyses and funding priorities.

HMIS is a secure web-based software application designed to record and store client-level information on the characteristics and service needs of persons experiencing, or at risk of, homelessness. To comply with the requirements of CoC Program Interim Rule 24 CFR 578, each CoC is required to designate **one** HMIS. HUD expects CoCs to use HMIS data to track their progress in meeting CoC and project-specific performance goals, to support community-wide planning, and to identify how best to direct resources to prevent and end homelessness.

In addition to congressional direction relating to HMIS, HUD, other federal agencies, and the United States Interagency Council on Homelessness (USICH) are required under various statutory authorities and congressional direction to collect information about the nature and extent of homelessness. Both individually and as a whole, these provisions provide statutory imperatives for collecting comprehensive data on persons experiencing homelessness and their needs.

The 2004 HMIS Data and Technical Standards Final Notice and the 2011 HMIS Requirements Proposed Rule require the development and implementation of comprehensive HMIS policies and procedures. This manual is intended to provide the Nashville-Davidson County CoC with a set of standardized HMIS policies and procedures. Additionally, this manual serves to document how the CoC is implementing (or is in the process of implementing) the HMIS requirements established by HUD. The manual covers the current processes and procedures, as well as processes that are still in development by the HMIS Oversight Committee of the CoC. The manual is based on guidance provided by HUD and local input from a variety of stakeholders, including homeless service providers and persons with lived experience of homelessness.

Section 2: HMIS Lead Agency Roles & Responsibilities

Metro Social Services (**MSS**) currently acts as the **HMIS Lead Agency** for the Nashville-Davidson County Continuum of Care. This section contains a brief overview of the major roles and responsibilities of the HMIS Lead Agency. The roles and responsibilities listed here are intended to provide a general overview and should not be taken as exhaustive or all-encompassing. In practice, the HMIS Lead Agency may assume additional roles and responsibilities as needed to support the work of the Collaborative Applicant and efforts of the Continuum of Care to prevent and end homelessness.

HMIS Lead Agency Roles

While the CoC Program Interim Rule assigns ultimate responsibility for HMIS to the CoC, the management of HMIS is delegated to the HMIS Lead Agency.

By stressing the importance of shared accountability for HMIS, HUD expects that CoCs will help to strengthen HMIS by:

1. Leveraging greater provider participation and higher data quality;
2. Reinforcing the role of HMIS in supporting other CoC functions; and
3. Ensuring HMIS Policies and Procedures are consistent with CoC goals.

HMIS Lead Agency Responsibilities

Key HMIS Lead Agency responsibilities include:

- Technical support for HMIS users and communication with the HMIS vendor (see Section 8: Technical Support);
- End user training (see Section 7: Training);
- Data quality monitoring (see Section 10: Data Quality);
- Ensuring privacy, safety, and security requirements are met (see Section 6: Privacy, Safety & Security);
- Obtaining and retaining necessary provider and end user agreements (see Section 3: HMIS Member Agency Roles & Responsibilities and Section 4: User Administration)
- System-wide reporting on performance measures for local, state and national initiatives (see Section 11: Performance Measurement); this includes working with the Collaborative Applicant to submit HUD-required reports such as the Longitudinal Systems Analysis (LSA), System Performance Measures (SPMs), Housing Inventory Count (HIC), and Point in Time Count (PIT); and
- Staffing the HMIS Oversight Committee.

Section 3: HMIS Member Agency Roles & Responsibilities

HMIS Member Agency refers to any participating provider whose staff enter data into HMIS. All Member Agencies receiving funding from HUD are mandated to participate in HMIS by contract, as are Member Agencies receiving some other types of federal, state, and local funding (e.g., VA, HHS, etc.). For other agencies providing housing-related services, participation is strongly encouraged by the Continuum of Care. Victim service providers are prohibited from entering data into HMIS. Victim service providers that receive funds requiring participation in HMIS must instead use a comparable database (see Section 9: Data Collection.)

Policy 3.1: The HMIS Lead Agency, in consultation with the Continuum of Care's HMIS Oversight Committee, is responsible for determining which organizations may participate in HMIS.

Procedure: Any organization that provides housing-related services may qualify to participate in HMIS. Organizations requesting to participate in HMIS must engage in an initial conversation (and, if necessary, a site visit) with the HMIS Administrator or other designated HMIS staff. During this conversation, HMIS staff will document the goals of the prospective HMIS Member Agency (i.e. what the agency wants to accomplish by participating in HMIS); review the required data elements; and review the HMIS Policies and Procedures, the HMIS Member Agency Agreement, and current HUD HMIS regulations (e.g., 2004 HMIS Data and Technical Standards Final Notice). This preliminary assessment also allows HMIS staff to properly assess the prospective HMIS Member Agency workflow and user needs; specific

implementation concerns; and any constraints or risks that will need to be mitigated by the prospective HMIS Member Agency prior to going live. HMIS staff will also evaluate the ability of the prospective Member Agency to abide by current HUD HMIS regulations, and any agencies deemed unable to abide by these regulations will be ineligible to participate in HMIS.

The HMIS Member Agency Agreement, developed by the HMIS Lead Agency in consultation with the Continuum of Care's HMIS Oversight Committee, details the expectations for organizations that wish to participate in HMIS, including privacy, safety, and security requirements and limits on HMIS data entry and data use.

After conducting the initial assessment for a prospective Member Agency, the HMIS Administrator will present an overview of the findings from the site visit to the HMIS Oversight Committee and gather input from Committee members regarding the prospective HMIS Member Agency's request to participate in HMIS. Taking into account the results of the initial assessment and input from the Committee, the HMIS Lead Agency will make a determination of whether the prospective HMIS Member Agency should have the ability to participate in HMIS.

Policy 3.2: A qualified HMIS Member Agency representative is required to sign and abide by the terms of the HMIS Member Agency Agreement. The HMIS Member Agency is required to comply with the HMIS Policies and Procedures and with any laws that may affect disclosure of their clients' information (e.g., covered entities under the Health Insurance Portability and Accountability Act [HIPAA]).

Procedure: To participate in HMIS, Member Agencies must sign and agree to abide by the terms of the HMIS Member Agency Agreement, and all staff who will be entering data into HMIS must sign and abide by the terms of End User Agreements. The HMIS Member Agency Agreement is a legal contract between the HMIS Member Agency and the HMIS Lead Agency regarding specific HMIS guidelines and use. The agreement outlines details about the HMIS Member Agency's HMIS involvement and expectations of both parties. This agreement must be signed by authorized representatives of the HMIS Member Agencies and the HMIS Lead Agency. Both parties should retain copies of the fully executed agreement.

HMIS Member Agencies must also abide by the policies and procedures outlined in this document. Each HMIS Member Agency will receive an electronic copy of this document for distribution to staff who enter data into HMIS.

Finally, HMIS Member Agencies are responsible for ensuring that their participation in HMIS does not violate any existing laws or statutes governing the disclosure of client information for the clients they serve (e.g., HIPAA). Our current HMIS software is HIPAA-compliant and allows for additional privacy and security measures, as described below, in Section 6: Privacy, Safety & Security.

Corrective Action: If an HMIS Member Agency or any of its end users have violated any HMIS policy, HMIS staff will implement a Corrective Action Plan upon discovery of the violation. Any HMIS End User, HMIS Member Agency staff member, client, or other interested party may inform the HMIS Lead Agency of a potential violation by contacting the HMIS Administrator in writing. The message should describe, in as much detail as possible:

- A description of the suspected violation;

- A list of any particular individuals or HMIS Member Agencies suspected to be involved in the violation;
- Reference to a specific portion of the HMIS Policies & Procedures Manual or other governing document that the writer suspects has been violated; and
- The anticipated severity level of the violation (Minor, Major, or Severe). The list below includes examples of Minor, Major, and Severe violations. These examples are not intended to be an exhaustive list, and the HMIS Lead Agency will make the ultimate determination of the severity level of the violation.
    - *Minor Violations* include the absence of an HMIS User at a required training, unless prior arrangements have been made for receiving missed training; inability to reach minimum data quality standards; and lack of communication with HMIS Lead Agency regarding staffing changes that affect HMIS participation (e.g., new end users, change in primary Point of Contact, change in Security Officer, etc.).
    - *Major Violations* include repeated unresponsiveness of HMIS Member Agency to HMIS staff requests; failure to report security and privacy incidents; and lack of inclusion of the HMIS Lead Agency in the development of any data sharing agreements, business associate agreements, etc. executed by an HMIS Member Agency.
    - *Severe Violations* include security breaches and violations that pose an imminent risk to clients' rights, as outlined below in Section 5: Clients' Rights (e.g., end users sharing login information or leaving login information in plain view of others; improper access of client data beyond the scope outlined in the HMIS Policies and Procedures and Member Agency Agreement).

Additionally, the HMIS Lead Agency itself may identify violations of HMIS policy or other governing documents in the course of normal business. Upon discovery of a suspected violation, the HMIS Administrator will investigate and, if necessary, require the HMIS Member Agency responsible for the violation to implement a Corrective Action Plan. The details of the plan will depend on the type and severity of the violation. Potential course of action include:

- Probation: The primary Point of Contact, or other appropriate staff member, at the HMIS Member Agency responsible for the violation will set up a one-on-one meeting with the HMIS Administrator to discuss the violation. During this meeting, a Corrective Action Plan will be developed and documented with clear expectations and a timeline for resolution/correction of the violation. The Member Agency will be placed on probation for a minimum of 90 days, during which time additional monitoring/auditing may be performed by the HMIS Lead Agency.
- Suspension: In the event of a Severe violation or initial failure to meet the expectations outlined in the Corrective Action Plan during the probationary period, the HMIS Administrator will suspend access to HMIS for all end users at the Member Agency responsible for the violation. The HMIS Member Agency will receive a written notice of the suspension, including the reasoning and effective date of the suspension. Appropriate staff from the HMIS Member Agency will meet with HMIS staff to discuss the violation and develop a Corrective Action Plan, as described above. If the Member Agency meets the deliverables within the agreed upon time frame, end users at the

Member Agency will regain access to HMIS, and the Member Agency will enter a 90-day probationary period, as described above.

- Termination: In the event of *repeated* failures to meet the expectations outlined in the Corrective Action Plan for *Minor/Major* violations, or *initial* failure to meet the expectations outlined in the Corrective Action Plan for *Severe* violations, the HMIS Member Agency will forfeit their ability to participate in HMIS. The HMIS Member Agency will receive a written notice of termination, including the reasoning and effective date of termination. HMIS Member Agencies whose participation is terminated may have the ability to renew their participation, but must undergo the same process as a first-time prospective HMIS Member Agency. The HMIS Lead Agency will take the previous termination into consideration when making a determination regarding the prospective Member Agency's request to regain access to HMIS.

Policy 3.3: Pursuant to the 2011 Homeless Emergency Assistance and Rapid Transition to Housing (HEARTH): Proposed Rule for HMIS Requirements, each HMIS Member Agency must designate an HMIS Security Officer.

Procedure: Member Agencies should work with the HMIS Administrator to determine the most appropriate staff member to serve as the HMIS Security Officer. For many Member Agencies, an existing compliance/privacy officer will be the most appropriate person to serve as the HMIS Security Officer. The HMIS Security Officer is responsible for ensuring compliance with applicable security standards.

Policy 3.4: Each Member Agency is required to designate a Primary Point of Contact (POC) for the Agency.

Procedure: Member Agencies should work with the HMIS Administrator to determine the most appropriate staff member to serve as the POC. If an agency utilizes HMIS for multiple programs whose staff do not overlap, the agency may need to designate more than one POC. We acknowledge that POCs will have varying levels of experience and understanding of the more advanced aspects of HMIS. Accordingly, we have designated the following minimum requirements and additional opportunities for POCs.

The POC is *required* to:

- Sign both an End User Agreement and a Primary POC Agreement, after attending an initial training with HMIS staff
- Enforce the HMIS Policies and Procedures;
- Attend an annual Primary Point of Contact Training;
- Maintain current user license inventory by informing the HMIS Administrator of any changes in usership within five business days of the change;
- Notify the HMIS Administrator within 15 days of any change to the HMIS Security Officer;
- Ensure that end users are aware of any procedural changes and that end users attend any required trainings;

- Act as the liaison to the HMIS Administrator for technical support needs of end users at their agency;
- Enforce HMIS End User Agreements and inform the HMIS Administrator of any suspected violations within 24 hours;
- Ensure the HMIS Privacy Notice is posted in a visible area of the Agency and communicated in language understandable by clients;
- Enforce data collection, entry, and quality standards;
- Ensure that end users are using the correct HMIS-related forms and following the most current HMIS procedures and workflow;
- Authorize, and work with HMIS Administrator to schedule, HMIS end user trainings;
- Inform HMIS staff of any project change, including new projects or projects ending, at least five business days prior to the anticipated change; and
- Inform HMIS staff of any changes in bed or unit inventory (for residential projects), as described below, in Section 9: Data Collection.

The POC may also perform the following roles, after receiving additional subject-specific trainings:

- Run agency-specific data quality reports;
- Act as the first tier of technical support for end users at their agency; and
- Participate in Train-the-Trainer opportunities.

Section 4: User Administration

Policy 4.1: All HMIS end users should have had a background check prior to receiving access to HMIS.

Procedure: Among the anticipated changes of the 2011 HMIS Requirements Proposed Rule is the requirement that all HMIS end users have a background check in order to access HMIS. The Nashville-Davidson County CoC recognizes the importance of protecting the privacy and confidentiality of client information. As such, HMIS Member Agencies are required to conduct background checks on all staff who will have access to HMIS.

Policy 4.2: HMIS access will not be granted to any prospective HMIS end user who is found to have entered a plea of *nolo contendere* (no contest) or who has been found guilty of the following:

1. Any fraud (including identity theft);
2. Any stalking-related felony crimes; or
3. Any sex offense.

Procedure: HMIS Member Agencies should not risk the privacy and confidentiality of client information by allowing any individual with a history of fraud or stalking-related felony crimes. Prior to requesting access to HMIS for a prospective end user, the HMIS Member Agency should ensure that the user does not have a history of fraud or stalking-related felony crimes. Current staff members with access

to HMIS should also be evaluated by the HMIS Member Agency using the guidance provided in this manual. If the HMIS Lead Agency becomes aware of any history of fraud or stalking-related felony crimes of any current HMIS end user, the HMIS Administrator will immediately revoke the user's access to HMIS.

Policy 4.3: Any prospective HMIS end user who was a previous client of the same project where he or she now intends to work must not have resided at the facility or been a project participant in the last six months prior to gaining access to HMIS.

Procedure: An HMIS user should never have access to detailed information on project/service participants who may have received services at the same time as the HMIS user. Any HMIS Member Agency that violates this policy is putting client information at risk of a privacy and confidentiality breach. Upon discovery of this practice, the HMIS Administrator will immediately revoke the end user's access to HMIS.

Policy 4.4: Except under very limited circumstances, no active member of law enforcement or detention/corrections staff will be granted access to HMIS.

Procedure: To protect the privacy and confidentiality of clients entered into HMIS, active members of law enforcement will not be granted access to HMIS. *Limited* exceptions may be negotiated when there is a project with direct involvement in an active homeless jail diversion and/or prison release project. These exceptions would require approval by the HMIS Oversight Committee, and an agreement must be executed that includes a statement that HMIS use is (1) limited to the purpose for which it was intended; and (2) is only for work with clients involved in that particular project.

Policy 4.5: Prospective HMIS end users must sign and adhere to an HMIS End User Agreement in order to have and maintain access to HMIS.

Procedure: Prior to being granted access to HMIS, all prospective end users must sign an HMIS End User Agreement. This document outlines the roles and responsibilities required for an end user to have and maintain access to HMIS. Any HMIS end user who violates the HMIS End User Agreement will have their license inactivated and will be required to attend additional training in order to regain access to HMIS.

Policy 4.6: The HMIS Lead Agency is responsible for administering HMIS end user licenses and providing initial training for prospective end users.

Procedure: Due to the amount of personally identifying information and the confidential nature of the information contained in HMIS, only the HMIS Lead Agency may grant access to a prospective HMIS end user. In order to receive a user license, the prospective end user must not violate the above policies 4.1 through 4.4.

The HMIS Administrator will assign the appropriate level of access to end users based on their role in the Member Agency. End users will be assigned to the lowest level of access required to perform their work duties. The primary Point of Contact (POC) should inform the HMIS Administrator of the need for any changes in access that may result from a change in the end user's job responsibilities (see Section 3: HMIS Member Agency Roles & Responsibilities).

The primary POC at each HMIS Member Agency is responsible for notifying the HMIS Administrator of any new users, change in user access, or license revocation as described in Section 3: HMIS Member Agency Roles & Responsibilities. The HMIS Administrator is ultimately responsible for issuance, maintenance, and inactivation of user licenses.

In addition to the potential reasons for inactivation of an end user license described in the above policies, the HMIS Administrator has the discretion to inactivate end user licenses for any of the following reasons:

1. *Inactivity*. HMIS end users must allow no more than 60 days between login sessions on the live site to keep their license active. The HMIS Administrator will inactivate the license of any HMIS user who has not logged in for 60 days or more. The user may be required to attend additional training prior to regaining access.
2. *Consistently poor data quality*. As described below, in Section 10: Data Quality, good data quality is critical to the health of HMIS. HMIS users who demonstrate consistently poor data quality, as determined by the HMIS Administrator, may have their license inactivated and be required to additional training prior to regaining access.
3. *Lack of attendance at required trainings*. Any end user who fails to attend a required training will have their license inactivated and will be required to make up the training to regain access.
4. *Violations of the HMIS Policies and Procedures*. Any end user found to be in violation of the HMIS Policies and Procedures will have their license inactivated and be required to attend additional training prior to regaining access.

In the event that the HMIS Administrator must inactivate an end user's license, the HMIS Administrator will inform the end user and the primary POC for the Member Agency. If the user still needs access to HMIS, the HMIS Administrator will work with both the end user and the primary POC to develop a plan for reactivation of the license.

Section 5: Clients' Rights

The Nashville-Davidson County Continuum of Care recognizes the importance of promoting and respecting clients' rights in the administration of HMIS. First and foremost, we acknowledge that the client ultimately retains ownership of any identifiable client-level information stored within HMIS. All data provided by the client, then, ultimately "belong" to the client.

Protection of clients' rights is vital to the provision of services, the strength of data quality, and the overall health of HMIS. The policy guidance provided in this document is designed to foster data sharing among HMIS Member Agencies; this model relies heavily on the enumeration and protection of clients' rights.

There is an important distinction between data *storage* in HMIS and data *sharing* in HMIS, which affect the policies in this section. Simply put, **data storage** refers to the use of HMIS for the purposes of housing client data. For the purposes of this document, we use the term *data storage* to refer to client data that is only visible to the HMIS Member Agency entering the data and is *not* shared among multiple HMIS Member Agencies.

Data sharing is the authorization for multiple HMIS Member Agencies to view the same client data within a single HMIS implementation. The Nashville-Davidson County CoC wishes to promote data sharing in HMIS because of the many benefits of data sharing at the client-, end user-, and system-level, such as:

- Limiting the number of times clients must recount their stories, reducing trauma;
- Improving collaboration among providers;
- Facilitating the day-to-day processes that allow staff at various agencies to easily collaborate and more effectively stabilize clients in appropriate housing with the appropriate wraparound services and supports;
- Improving the flow of information among agencies, allowing them to provide faster and better services to clients;
- Reducing duplicative data collection and data entry for end users;
- Streamlining housing and service referrals; and
- Getting higher quality, more comprehensive data that support more effective evaluation of programs and processes and stronger funding requests.

Data sharing in HMIS requires a robust privacy and data security framework (with accompanying training and ongoing monitoring), client consent to share data, and client ability to review and correct data. This section addresses the latter two items; privacy and security are addressed in Section 6: Privacy, Safety & Security.

Client Consent

Policy 5.1: HMIS Member Agencies must obtain the appropriate level of consent (i.e. informed consent or a written release of information) from all clients for whom they are entering or accessing client data in HMIS.

Procedure: The level of consent required varies depending on the circumstances of data collection and data entry. If a household with multiple members is being served, guardians are able to consent to HMIS data storage and sharing for their dependents under the age of 18. However, each household member age 18 or older must provide their *own* consent for data storage or sharing in HMIS.

- **Informed consent** refers to a process for getting permission before collecting and storing information in HMIS. The 2004 HMIS Data and Technical Standards Final Notice leaves open the option of using oral consent as a basic minimum for obtaining consent, but written consent is preferable.

- A signed Release of Information is a document that allows the client to decide *what* information they want to share from their file, *who* they want to share the information with, *how long* the release is valid, and *under what circumstances* data are shared. While informed consent is sufficient for data *storage* in HMIS, a signed Release of Information is required for data *sharing*. The original signed Release of Information should be kept on file with the HMIS Member Agency where it was signed, and an electronic copy should be uploaded in HMIS.

Policy 5.2: Client refusal to provide consent for data sharing in HMIS will not affect their ability to receive services from an HMIS Member Agency.

Procedure: Clients who refuse to provide consent for data *sharing* for themselves or their dependent household members in HMIS (i.e. through a signed Release of Information) cannot be denied services from an HMIS Member Agency on the basis of this refusal. However, there are some instances in which refusal to provide consent for data *storage* in HMIS may affect a client's and/or their household's ability to receive some types of services, depending on the requirements of the funder. For instance, refusal to provide consent for data entry into HMIS can prevent a veteran from receiving services funded by the VA's Supportive Services for Veteran Families (SSVF) program. These non-negotiable funder decisions are outside of the purview of this document.

Policy 5.3: All clients who agree to participate in HMIS have the option to revoke or change their permission for data sharing in HMIS at any time.

Procedure: Clients who choose to revoke their permission for data sharing, or to change the data they choose to share or the agencies with which they choose to share that data in HMIS, must complete a new written Release of Information to request these changes in sharing permissions. Within two business days of receiving the updated Release of Information, the HMIS Member Agency collecting the updated Release of Information should:

(1) Upload the updated Release of Information in HMIS, and
(2) Notify HMIS staff that the data sharing permissions need to be changed or revoked by e-mailing the HMIS Help Desk: HMISHelp@nashville.gov.

Within three business days of receiving this notification from HMIS Member Agency staff, the HMIS Administrator will modify the visibility of the client record in HMIS to be consistent with the new Release of Information. The HMIS Administrator will then provide confirmation of these changes to the HMIS Member Agency staff.

The client record will be modified to reflect the updated data sharing permissions within a maximum of five business days of the client completing an updated Release of Information. Note that revocation or modification of consent to share data is *not* retroactive; so, the decision to revoke or modify consent for data sharing is only effective as of the date the client record is closed in HMIS. Data entered prior to the record being closed can still be viewed and shared under the data sharing permission that was active at the time the data were entered.

Client Access to Information

Policy 5.4: All clients entered into HMIS have a right to view information within their electronic HMIS record and to have a copy of that information provided to them.

Procedure: If an HMIS Member Agency has a written policy for providing copies of their paperwork or data collection to clients, the HMIS Member Agency may follow its procedures to allow for providing copies of the paperwork they completed with the client.

Clients may also request a copy of all information that has been entered into their record in HMIS, which would include data entered into their HMIS record by *any* HMIS Member Agency. To request this information, the client can either contact the HMIS Help Desk directly at HMISHelp@nashville.gov, or request that a staff member at an HMIS Member Agency do so on their behalf. The HMIS Administrator will review the request and, in consultation with the client, determine the appropriate method of providing this information to the client (e.g., through secure e-mail, written printout provided to client, etc.).

Filing a Grievance

Policy 5.5: Clients have a right to file a grievance with the HMIS Lead Agency about suspected violations of HMIS policies and procedures; or laws governing the storage of, sharing of, and access to data in HMIS.

Procedure: Clients who suspect that an HMIS Member Agency or end user has violated HMIS policies and procedures or other governing documents should follow the process described above, in the *Corrective Action* portion of Policy 3.2. In cases where a client leaves one HMIS Member Agency to receive services from another HMIS Member Agency and reports a suspected violation by the first agency, the new HMIS Member Agency may file a grievance on the client's behalf, as long as the client grants their permission to do so.

Once the HMIS Lead Agency has completed their investigation of the suspected violation and determined a course of action, all parties involved (including the client who filed the grievance) will be notified in writing. If the client is not satisfied with the findings of the investigation or the proposed course of action to address the violation, the client may submit a grievance in writing to the U.S. Department of Housing and Urban Development. If deemed necessary by the client, the client may take a grievance straight to the U.S. Department of Housing and Urban Development.

Section 6: Privacy, Safety & Security

As described above, in Section 5: Clients' Rights, data sharing in HMIS requires a robust privacy and data security framework. Pursuant to the 2004 HMIS Data and Technical Standards Final Notice, the standards described in this section seek to protect the confidentiality of personal information while allowing for reasonable, responsible, and limited uses and disclosures of data. The possible allowed uses and disclosures allowed by the Data and Technical Standards Final Notice include: 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 Protected Personal Information (PPI).

In the 2004 HMIS Data and Technical Standards Final Notice, HUD lays out a two-tiered approach to privacy and security, with baseline standards required of any organization along with additional protocols or policies that organizations may choose to adopt to further protect the privacy and security of information collected through HMIS. This approach recognizes the broad diversity of organizations that participate in HMIS and the differing programmatic and organizational realities that may demand a higher standard for some activities. HMIS implementations are required to have to have a disaster recovery plan. HMIS software is covered by the software vendor's Disaster Recovery Plan. Database backups occur nightly, and a one-month backup history is stored. The policies in this section reflect the baseline standards required for all HMIS Member Agencies.
Note that ***personal protected information (PPI)*** refers to any information maintained by an HMIS Member Agency about a living client that: (1) identifies, either directly or indirectly, a specific individual; (2) can be manipulated by a reasonably foreseeable method to identify a specific individual; or (3) can be linked with other available information to identify a specific individual.

Policy 6.1: HMIS Member Agencies must comply with all federal, state, and local laws, standards, and regulations regarding privacy, safety, and security.

Procedure: HMIS Member Agencies are required to understand and comply with any and all federal, state, and local laws, standards, and regulations that govern privacy, safety, and security (e.g., covered entities under HIPAA and/or 42 CFR Part 2). Victim service providers are prohibited from entering PPI into HMIS for their clients, as described below, in Policy 9.4. HMIS staff should conduct an annual security review for HMIS Member Agencies in accordance with Section III of the 2011 HMIS Requirements Proposed Rule.

Policy 6.2: HMIS Member Agencies must comply with the baseline security standards described in the 2004 HMIS Data and Technical Standards Final Notice.

Procedure: The 2004 Data and Technical Standards Final Notice lays out a set of baseline standards for system security, application security, and hard copy security. These standards are summarized below.

System Security: The system security standards apply to all systems where PPI is stored, including, but not limited to, an HMIS Member Agency's networks, desktops, laptops, and servers.

User Authentication. HMIS end users are required to access HMIS using a username and password that is only known to that end user. Passwords must be at least eight characters long and meet reasonable industry standard requirements. HMIS end users may not share this information or store it in writing in any publicly accessible location. Users must choose a new password every 45 days.

Virus Protection. HMIS Member Agencies must protect their systems from viruses by using commercially available virus protection software. Virus protection must include automated scanning of files as they are accessed by users.

Physical Access to Systems with Access to HMIS Data. To restrict access to HMIS data to only authorized end users, workstations where HMIS data are collected should automatically turn on a password protected screensaver after a short time when the workstation is not in use. HMIS users utilizing laptops to collect data in the field should maintain physical control of the laptop at all times.

System Monitoring. HMIS Member Agencies must use appropriate methods to monitor system security. Systems with access to any HMIS data must maintain a user access log (standard on most operating systems and web servers).

Application Security: The application security standards apply to HMIS software during data entry, storage, and review.

User Authentication. See above, in the system security standards.

Electronic Data Transmission. Data in HMIS are secured as they travel over the Internet and are stored on a centralized server. All HMIS transactions are fully encrypted using 128-bit encryption, the current industry standard. Additionally, the HMIS Lead Agency contracts with a HUD approved HMIS software vendor that secures the location of its server in a controlled hosting environment accessible only by the very few employees responsible for maintaining and supporting the system. The vendor's computers are also protected by firewalls to prevent unauthorized external access.

Hard Copy Security: HMIS Member Agencies must secure any paper or other hard copy containing PPI that is either generated by or collected for HMIS. This includes, but is not limited to: reports, data entry forms, and signed consent forms. HMIS Member Agency staff must supervise at all times any hard copy that is in a public area. When staff are not present, the information must be secured in areas that are not publicly accessible (e.g., locked rooms or locked filing cabinets).

Policy 6.3: HMIS Member Agencies must post a copy of the HMIS Privacy Notice prominently in areas of plain view of the public.

Procedure: HMIS Member Agencies are required to post an HMIS Privacy Notice that explains how PPI will be collected and used. HMIS Member Agencies must post a copy of the HMIS Privacy Notice in plain view of the public in their facilities and wherever HMIS data are collected. This may include waiting rooms, intake areas, lobbies, or screening or assessment areas. If the Member Agency maintains a public website, the HMIS Privacy Notice must also be posted on the website. Member agencies who collect data in the field or in non-traditional intake spaces are required to carry a copy of the HMIS Privacy Notice. Additionally, Member Agencies must provide a copy of the Notice to any individual who requests it. During an annual site visit, the HMIS Lead Agency will ensure that the Notice is posted in the appropriate area(s).

Policy 6.4: HMIS limits the visibility of data based on an end user's level of access and the type of consent provided by the client.

Procedure: As outlined in Section 4: User Administration, the HMIS Administrator will assign the appropriate level of access to end users based on their role in the Member Agency. End users will be assigned to the lowest level of access required to perform their work duties.

Additionally, the HMIS software utilizes a set of visibility settings that allow sharing of only those data elements for which the client has granted consent. Visibility settings may only be modified by HMIS staff.

Policy 6.5: In accordance with the 2004 HMIS Data and Technical Standards Final Notice, any HMIS Member Agency designated as a "covered entity" under HIPAA is exempted from the privacy and security standards described in this section.

Procedure: HUD recognizes that HMIS privacy and security standards should give precedence to the HIPAA privacy and security rules because: (1) the HIPAA rules are more finely attuned to the requirements of the healthcare system; (2) the HIPAA rules provide important privacy and security protections for protected health information; and (3) requiring a homeless service provider to comply with or reconcile two sets of rules would be an unreasonable burden. Any HMIS Member Agency that maintains personal information about a client that does not fall under the privacy and security standards in this section, because 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 by the HMIS privacy and security standards. 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 apply.

It is possible that part of a homeless service provider's operations may be covered by the HIPAA standards, while another part is covered by the HMIS standards. In that instance, the Member Agency should follow the standards laid out in this section.

Section 7: User Training

Policy 7.1: The HMIS Lead Agency establishes beginning, advanced, and ongoing training requirements for HMIS users.

Procedure: Prospective HMIS end users must participate in a mandatory Privacy & Security Training and complete an accompanying homework assignment. After reviewing the assignment for any major errors, HMIS staff will schedule a specific training for the end user, depending on the workflow they will be following for HMIS data entry (e.g., SSVF data entry, Coordinated Entry, etc.). Under no circumstances should anyone who has not received official training by HMIS staff have access to or use HMIS.

HMIS staff may offer additional training opportunities for more advanced users on topics such as reporting.

Policy 7.2: HMIS users must fulfill all initial and ongoing training requirements to gain and retain access to HMIS. The HMIS Administrator has the authority to inactivate or refuse to grant a license for any HMIS user who does not fulfill all training requirements.

Procedure: As described in Section 4: User Administration, failure to attend a mandatory training may result in inactivation of a user's license. The user may be required to make up the training, or attend additional training, to regain access.

Policy 7.3: The HMIS Lead Agency may hold periodic, mandatory meetings to discuss changes in HMIS Data Standards or HUD data requirements.

Procedure: Occasionally, the HMIS Lead Agency may find it necessary to hold mandatory meetings regarding changes that affect a broad range of users. HMIS staff will communicate this to primary POCs at Member Agencies, who will be responsible for ensuring that all appropriate staff members are in attendance.

Section 8: HMIS Technical Support

Policy 8.1: The HMIS Lead Agency provides a system that allows HMIS users to submit general HMIS related inquiries, questions related to training and workflow, and requests for technical assistance. HMIS staff respond to all inquiries in a timely manner.

Procedure: All HMIS related inquiries and requests for technical assistance must be submitted to the HMIS Help Desk: HMISHelp@nashville.gov. Every effort will be made to respond to messages submitted to the Help Desk within one business day. Normal working hours for HMIS staff are Monday through Friday, 7:30 am through 4:00 pm. After hours and weekend requests will be treated as if the request was received at the opening of the following business day.

Time required for resolution of the question or concern will vary depending on current staff capacity and the complexity and urgency of the request. To ensure that the inquiry is processed as quickly as possible, Member Agency staff should be as specific as possible. If the issue concerns a particular client record in HMIS, reference the HMIS ID in the message. If the issue has been noted across multiple client records, provide several examples of affected HMIS IDs. Vague inquiries that require clarification will take longer to resolve.

Policy 8.2: HMIS Member Agencies must submit all feature enhancement requests directly to the HMIS Lead Agency. HMIS Member Agencies should not, under any circumstances, communicate directly with the vendor regarding the Continuum of Care's HMIS implementation.

Procedure: The HMIS Lead Agency serves as the sole conduit for communication with the vendor regarding the Continuum of Care's HMIS implementation. Accordingly, all requests for feature enhancements should be submitted directly to the HMIS Help Desk, following the procedure detailed above.

Feature enhancement requests should include, at a minimum:

- A specific description of the problem (with examples, if applicable);
- A proposed solution; and
- Context regarding how and why the solution will be used.

Section 9: Data Collection

Policy 9.1: All client data entered into HMIS by the Member Agency should be that of clients receiving services.

Procedure: HMIS is not meant for clients who may benefit from services at a later date. In order to be entered into HMIS, clients must have received, or currently be receiving, services from an HMIS Member Agency. For the purposes of HMIS data collection, services include, but are not limited to: financial assistance, supportive services, housing, and referrals. If a client is a part of a household, other household members should also be entered into HMIS. Data on all members of the household should be entered individually, but tied together as a household.

Policy 9.2: HMIS Member Agencies are required to enter client level data in accordance with a set of predefined data standards.

Procedure: In order to meet minimum data entry standards, every HMIS Member Agency, *regardless of funding source*, is required to enter all Universal Data Elements (UDEs) as outlined in the most recent version of the HMIS Data Standards Manual. UDEs support the ability to record unique, unduplicated client records, establish participation in a project within a date range, and identify clients who meet the criteria for chronic homelessness.

Certain funding sources also require the collection of Program-Specific Data Elements (PSDEs) that provide additional information about the characteristics of clients, the services provided, and client outcomes. The HMIS Federal Partners have cooperatively developed these elements, which vary by program type and are outlined in the HMIS Data Standards Manual.

Policy 9.3: HMIS Member Agencies are required to maintain the most current bed and unit inventory for each of their HMIS-participating residential projects.

Procedure: Consistent with the HMIS Data Standards Manual, each HMIS must have an accurate record of bed and unit inventory for all residential projects, *regardless of funding source*. Accordingly, HMIS Member Agencies must notify the HMIS Administrator of the anticipated bed and unit inventory for new residential projects in HMIS. Additionally, HMIS Member Agencies must notify the HMIS Administrator of any changes in bed or unit capacity for existing residential projects. ***Residential projects*** include: emergency shelter (both year-round and seasonal), transitional housing, rapid rehousing, Safe Haven, permanent supportive housing, and other permanent housing.

To facilitate accurate recording of bed and unit inventory for existing residential projects, the HMIS Administrator requires HMIS Member Agencies to confirm bed and unit inventory in HMIS on a quarterly basis. For new residential projects, HMIS Member Agencies are required to report anticipated bed and unit inventory to the HMIS Administrator, so the project can be set up correctly in HMIS.

Policy 9.4: Victim service providers are prohibited from entering data into HMIS. Victim service providers that receive funds requiring participation in HMIS must instead use a comparable database.

Procedure: Consistent with Section 401(32) of the McKinney-Vento Act, ***victim service provider*** is defined as a private nonprofit organization whose primary mission is to provide services to victims of domestic violence, dating violence, sexual assault, or stalking. This term includes rape crisis centers, battered women's sheltered, domestic violence transitional housing programs, and others.

While victim service providers are prohibited from entering data into HMIS, aggregate data from these providers are necessary to evaluate system-wide performance of the Continuum of Care. As such, victim service providers receiving funding that requires participation in HMIS must use a comparable database, as provided under 24 CFR part 580. ***Comparable database*** means a database that is not the Continuum's official HMIS, but an alternative system that victim services providers may use to collect client-level data over time and to generate unduplicated aggregate reports based on the data. The

comparable database must, at a minimum, meet the standards for security, data quality, and privacy of the HMIS within the Continuum of Care.

Section 10: Data Quality

Data quality is critical to the success of HMIS. Good data quality helps to ensure that reports at both the provider and system level offer complete and accurate representations of the services being provided, clients benefiting from those services, and relevant client outcomes. Adherence to data quality standards will enable our community to better evaluate efforts to end homelessness and will help to secure and sustain funding in order to better serve people experiencing housing crises in Nashville-Davidson County.

In 2017, HUD released a CoC Data Quality Brief as part of a series of resources to support system improvement. The definitions of the three key facets of data quality (completeness, accuracy, and timeliness) provided below come from this brief. The HMIS Lead Agency, in consultation with the Continuum of Care's HMIS Oversight Committee, will establish a Data Quality Plan that lays out specific benchmarks for completeness, accuracy, and timeliness. These benchmarks may vary by project type and are subject to change as needed.

Policy 10.1: The HMIS Lead Agency will evaluate the completeness of HMIS Member Agency data.

Procedure: ***Completeness*** is the degree to which all required data are known and documented in HMIS. Partially complete or missing data can negatively affect the ability to provide comprehensive, person-centered services and increase the amount of time it takes to help clients identify and access appropriate housing resources. At least once per quarter, HMIS staff will provide a data completeness report to each Member Agency, developed by the HMIS vendor. HMIS Member Agencies must review these reports and take steps to correct or explain any incomplete data.

At least once a year, the HMIS Administrator will conduct site visits with every HMIS Member Agency, *regardless of funding source*. At this visit, the HMIS Administrator will review the completeness of the Member Agency's projects for the previous year and develop a Corrective Action Plan with the Member Agency, if needed, to correct any outstanding data completeness issues.

Policy 10.2: The HMIS Lead Agency will evaluate the accuracy of HMIS Member Agency data.

Procedure: ***Accuracy*** is the degree to which data reflect the reality of clients and services. Accuracy depends on the client's ability to provide the correct data and staff's ability to document and enter data correctly into HMIS. HMIS training and technical support procedures, detailed in Sections 7 and 8 above, are designed to enhance staff's ability to accurately collect and enter data.

At the annual site visit with each HMIS Member Agency, the HMIS Administrator will request access to a random sample of files of clients whose data have been entered into HMIS. The HMIS Administrator will evaluate accuracy of HMIS data by comparing the data in the charts to data entered into HMIS.

Policy 10.3: The HMIS Lead Agency will evaluate the timeliness of HMIS Member Agency data.

Procedure: *Timeliness* is the degree to which data are collected and available when needed. Entering data in a timely manner can reduce human error caused by too much time elapsing between data collection and entry. Timely data entry also ensures that data are accessible when needed (e.g., monitoring purposes, reporting to funders, responding to requests for information).

At least once per quarter, HMIS staff will provide a data timeliness report to each Member Agency, developed by the HMIS vendor. HMIS Member Agencies must review these reports and take steps to improve or explain issues with timeliness. Additionally, at the annual site visit, the HMIS Administrator will review timeliness of data entry for the Member Agency's projects and, if needed, develop a Corrective Action Plan with specific steps to improve timeliness of data entry.

Policy 10.4: HMIS Member Agencies will be responsible for promptly addressing any data quality concerns identified by the HMIS Lead Agency.

Procedure: As described above, the HMIS Administrator will provide several opportunities throughout the year for Member Agencies to review and correct issues with data quality. HMIS Member Agencies or HMIS users with consistently poor data quality, as determined by the HMIS Administrator on the basis of the benchmarks set in the HMIS Data Quality Plan, may forfeit their ability to access HMIS until they complete additional training and develop a Corrective Action Plan to remedy data quality issues.

Section 11: Performance Measurement

Performance measurement is key to our community's efforts to prevent and end homelessness. Ongoing performance measurement at the project, agency, and system levels can be used to inform system planning activities and resource investments, inform local evaluation criteria, and monitor the results of project and system-wide changes. HMIS serves as one of the largest sources of homelessness data in Nashville-Davidson County. As such, HMIS data are critical to assessing progress toward preventing and ending homelessness. Careful consideration of the results of performance measurement can help identify gaps in data and services and reveal significant information about how well homeless assistance programs are functioning as a whole and where improvements are necessary.

Policy 11.1: HMIS data will be used to measure progress toward HUD System Performance Measures (SPMs).

Procedure: HUD has developed seven system-level performance measures to help communities gauge their progress in preventing and ending homelessness:

1. Length of time persons remain homeless;
2. Returns to homelessness after exiting to permanent housing destinations;
3. Number of persons experiencing homelessness;
4. Jobs and income growth for persons experiencing homelessness in CoC-funded projects;
5. Number of persons experiencing homelessness for the first time;

6. Homelessness prevention and housing placement of persons defined by Category 3 of HUD's homeless definition in CoC-funded projects (currently not applicable for Nashville-Davidson County CoC); and
7. Successful housing placements.

The purpose of these measures is to provide a more complete picture of how well a community is preventing and ending homelessness. The performance measures are interrelated and, when analyzed relative to each other, provide a more complete picture of system performance. Importantly, the value of the SPMs depends in part on (1) the quality of HMIS data, and (2) HMIS coverage across all homeless service providers in the CoC. If HMIS data quality is low and/or HMIS coverage is lacking, the SPMs will not be as useful. To this end, the HMIS Lead Agency will continue efforts to increase bed coverage in HMIS by encouraging providers that do not currently enter data into HMIS, and those that enter data for only a portion of their clients served, to begin or expand their HMIS participation. The HMIS Lead Agency does not bear sole responsibility for increasing bed coverage in HMIS; the Collaborative Applicative and Nashville-Davidson County Continuum of Care Homelessness Planning Council must also serve as leaders in this effort.

HUD requires CoCs to submit their SPMs annually. The HMIS Lead Agency works with the Collaborative Applicant to compile and submit SPMs to HUD through the HUD Exchange. HMIS Member Agencies are responsible for promptly responding to requests from the HMIS Lead Agency regarding data issues that may affect SPMs. To reduce the annual burden and make this process more efficient, HMIS Member Agencies should work throughout the year with the HMIS Lead Agency to ensure that their data quality is high and that they are aware of any changes in data entry requirements (see Section 10: Data Quality).

Policy 11.2: HMIS data will be used to support local strategic priorities.

Procedure: In addition to using HMIS data for HUD SPMs, HMIS data should be used to support any additional local strategic priorities and to measure the performance at the agency and project levels (e.g., emergency shelter, transitional housing, etc.). This may include, but would not be limited to, priorities identified in the Continuum of Care Strategic Plan, the Written Standards Committee, and the Performance Evaluation Committee (PEC) annual ranking and rating process.

The HMIS Lead Agency is responsible for overseeing the use of HMIS data to support local strategic priorities. While agencies may use their own HMIS data to gauge their agency's performance, any data beyond the agency level should come directly from the HMIS Lead Agency.