

Nashville-Davidson County HMIS Policies and Procedures

Proposed Policy and Procedure Revisions

New Revisions:

Cover Page/Table of Contents

- Rename Document: Nashville-Davidson County Continuum of Care HMIS Policies and Procedures Manual.
- Remove Metro Homeless Impact Division logo

Section 4: User Administration

- Removal of Policy 4.1: All HMIS End Users should have had a background check prior to receiving access to HMIS.
- Revision of Policy 4.2 (Now 4.1) to read as follows:

Policy 4.1: 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. Identity theft; or
2. Any stalking-related felony crimes

Procedure: The Nashville Davidson County CoC recognizes the importance of protecting the privacy and confidentiality of client information. In addition to the security policies detailed in section 6, it is vital that HMIS Participating Agencies should not risk the privacy and confidentiality of client information by allowing any individual with a history of identity theft or stalking-related felony crimes to access HMIS. Prior to requesting access to HMIS for a prospective end user, the HMIS Participating Agency should ensure that the user does not have a history of identity theft or stalking-related felony crimes. Current staff members with access to HMIS should also be evaluated by the HMIS Participating Agency using the guidance provided in this manual. The HMIS Lead Agency reserves the right to request a background check for any HMIS End User. If the HMIS Lead Agency becomes aware of any history of identity theft or stalking-related felony crimes of any current HMIS end user, the HMIS Administrator will immediately revoke the user's access to HMIS.

Agencies should uphold a secure digital environment in terms of data protection and legal compliance that protects against cyber stalking and identity theft.

- Revision of New Policy 4.X (to be placed after the current Policy 4.4) to read as follows:

Policy 4.x: Prerequisite Computer Competencies

Procedure: Every HMIS end user is required to have basic computer skills prior to being granted access to HMIS. Prior to requesting a license, the HMIS Partner Agency should confirm the end user have the basic computer competency skills necessary for the handling of Personally Identifiable Information. HMIS Partner

Agencies should require all end users to obtain any computer competency skills they lack prior to requesting a license.

Minimum Computer Competency Skills include:

- Privacy: End users must be able to capture and remove PII from screenshots and understand the use of encryption to send sensitive data.
- Internet browser security: End users must be able to clear the internet browser cache and be familiar with privacy settings and password protocols.
- Software: End users must be familiar with collapsing/expanding navigation menus, file naming and file types, file uploading and attachment, and digital form functionality (e-signature and electronic submission).
- Hardware: End users must be familiar with locking workstations, and updating operating system.
- System Security: knowledge of common email scams (including phishing and hidden virus scams).

- Addition to the end of Policy 4.6: The HMIS Lead Agency is Responsible for administering HMIS End User licenses and providing initial training for prospective End Users, to read as follows:

Each Participating Agency entering data in HMIS will be allowed up to three licenses for End Users per project. Projects not entering data will be allowed up to one license. A maximum of twelve total licenses will be allowed per Participating Agency.

If a Participating Agency believes they will need more than the allowed number of licenses the request will be considered on a case by case basis by the HMIS Lead Agency. The decision of whether or not to grant additional licenses will be made based on the size and scope of the program, number of entries and/or updates in the system made by the Agency's End Users, the Partner Agency's data quality, and availability of licenses within the system. The number of licenses granted to the Participating Agency is contingent upon the total number of available licenses.

Section 5: Clients' Rights

- Revision of New Policy 5.X (to be placed after the current Policy 5.2) to read as follows:

Policy 5.3 – HMIS Participating agencies are responsible for maintaining security and confidentiality of all client's personal and identifying information contained within the HMIS with respect to data sharing.

Procedure: Any personal identifying information in HMIS belonging to clients who have consented to share their information can be shared with only the entities listed and purposes stated in the Nashville – Davidson County HMIS: Public Privacy Notice and Release of Information (ROI). HMIS Participating agencies and end users should not use, share, disclose or release any personal identifying information obtained from HMIS of clients who do not consent to share their data with anyone or any entities that that does not have access to HMIS which would include but are not limited to:

1. Other HMIS Participating Agencies.
2. Organizations and agencies not permitted or approved by the HMIS Lead Agency like law enforcement, courts, detentions/corrections staff etc.
3. Individuals like family members or friends.
4. Elected officials.
5. Artificial Intelligence (AI) tools that include but not limited to Chat GPT, Perplexity, Fireflies, Google Assistant, Amazon Alexa, and Siri.

6. Social media platforms, newspapers, news broadcasting channels, and any other journalism or media entity.

Previously Discussed Revisions

Throughout Document

- Change “HMIS Member Agency” to “HMIS Participating Agency” where applicable

Section 1: Introduction

- Remove reference to the 2011 HMIS Requirements and Proposed Rule in fourth paragraph

Section 2: HMIS Lead Agency Roles and Responsibilities

- Replace “Metro Social Services” with “Office of Homeless Services” as the HMIS Lead Agency
- Add language referring to conflicts of interest.

The HMIS Lead Agency is subject to policies and procedures as outlined within the Nashville-Davidson County Continuum of Care Charter including, but not limited to, section 9 item E on conflicts of interest.

Section 3: HMIS Member Agency Roles and Responsibilities

- Policy 3.4 under Point of Contact requirements, edit point 3 to read:

Attend all Primary Point of Contact Meetings and Trainings.

- Add Policy 3.5

Policy 3.5: HMIS Partner Agencies are responsible for the actions of their HMIS End Users.

Procedure: HMIS Partner Agencies are responsible for assessing the appropriateness of any potential HMIS End User within the agency. Potential End Users must be considered not only to have the technical skills required to work within the HMIS system, but must also to be

- Trustworthy with sensitive, confidential, and client identifying information
- Ethical in behavior and practices
- Safety and Security conscious
- Reliable
- In good standing with their employer and within the HMIS community

HMIS Partner Agencies will not submit requests for HMIS access for any individual who pose a known or believed threat to the integrity of the HMIS system and/or the data contained within the system.

- Add Policy 4.x above Policy 4.3

Policy 4.x: HMIS end user access is dependent on the HMIS end user's employment with the HMIS Partner Agency.

Procedure: HMIS end users are immediately prohibited from accessing the HMIS for any reason upon termination of employment with the HMIS Partner Agency. HMIS end user access of the HMIS after termination of employment could result in the HMIS end user being barred from any future access to the HMIS and/or violation findings against the HMIS Partner Agency.

HMIS end users terminating employment with one HMIS Partner Agency in order to obtain employment with another HMIS Partner Agency must immediately discontinue use of their previous HMIS log in and be re-submitted for licensure by the HMIS Partner Agency that currently employs the end user.

- Adjust language in Policy 4.6 on item 1. *Inactivity* from “The user *may be* required to attend additional training prior to regaining access.” To “The user *will be* required to attend additional training prior to regaining access.”

Section 6: Privacy, Safety, and Security

- Remove reference to the 2011 HMIS Requirements and Proposed Rule in Policy 6.1
- Policy 6.3 Add to existing Policy:

Disposal: The HMIS Partner Agency agrees to commit itself to security protections consistent with HMIS requirements by agreeing to dispose of documents that contain identifiable client level data. Methods may include:

- Shredding paper records
- Deleting any client identifying information from all equipment before disposal
- Deleting any copies of identifiable client level data from the hard drive of any machine before transfer or disposal of property.

Section 7: User Training

- Policy 7.1 Remove language that says:

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.).

and rewrite sentence to read:

Prospective HMIS End Users must participate in a mandatory training process that includes online training hosted on our Learning Management System and training exercises. This training process includes completion of a mandatory Privacy & Security Training.

Section 9: Data Collection

- Add Policy 9.5

Policy 9.5: Data Collection and entry can be completed through a data import.

Procedure: HMIS Partner Agencies may choose to enter data into HMIS through an import of the data within their own agency database. The HMIS Partner Agency must still complete and sign the HMIS Participating Agency Agreement and adhere to the HMIS policies and procedures.

There may be fees related to the creation of the import functionality. Pricing is dependent on the HMIS vendor. Participating Agencies wishing to explore this option must submit a request to the HMIS Lead Agency through the HMIS help desk. The request must include the scope of the potential data import.

Once the import process is established, the HMIS Partner Agency will be required to complete imports in a regular and timely manner.