Miami-Dade County Homeless Trust
Homeless Management Information System (HMIS)
Policies and Procedures Manual

Miami-Dade County Continuum of Care (CoC)

Approved by the Board 6.23.17
Revised 3/22/2024

Miami-Dade County Homeless Trust
Homeless Management Information System
Policies and Procedures Manual

Overview

The Miami-Dade County Homeless Trust (Homeless Trust) is the HMIS lead agency responsible for system administration and project management of the Miami-Dade County CoC's Homeless Management Information System (CoC HMIS). For implementation of its CoC HMIS, the Homeless Trust develops these CoC HMIS policy standards and subsequent procedures of data usage for all CoC HMIS users and user agencies. These P&Ps serve to better protect the confidentiality of all personal information entered into the HMIS while identifying the reasonable, responsible, and limited uses and disclosures of data, which comply with federal regulations set by the U.S. Department of Housing and Urban Development (HUD). Its purpose is to guide and clarify federal regulations for CoC agencies in their daily operations. It in no way, should serve as a substitute for any federal regulations outlined and updated by HUD in its Data and Technical Standards. All CoC agencies are responsible for maintaining their own compliance with federal regulations as well as any outside applicable regulations such as the Health Insurance Portability and Accountability Act (HIPAA) standards.

Table of Contents

I. Roles and Responsibilities

A. Homeless Trust

The Homeless Trust is the HMIS lead agency responsible for system administration and project management of the Miami-Dade County CoC's HMIS. The Homeless Trust will set and adhere to HMIS Policy and Procedures. The Homeless Trust will provide HMIS licenses to community stakeholders serving people experiencing or at risk of homelessness in Miami-Dade County, also known as covered homeless organizations (CHO). CHO's include Continuum of Care (CoC), Emergency Solutions Grant (ESG), Projects for Assistance in Transition from Homelessness (PATH), Runaway Homeless Youth (RHY) and the Veterans Administration (VA) who serve Miami-Dade County. The types of CoC-funded HMIS participating programs are Access Points, Street Outreach (SO), Emergency Shelter (ES), Transitional Housing (TH), Rapid Re-housing (RRH), Joint Component TH:RRH projects (TH:RRH), Permanent Supportive Housing (PSH), Other Permanent Housing (OPH) participating in the CoC Coordinated Entry System (CES), and standalone Support Service Only (SSO) projects providing services to people experiencing homelessness. Only CHO's funded by the CoC, ESG, PATH, RHY or VA who perform Street Outreach activities are provided access to the HMIS.

Some CHO's are provided HMIS access because they serve or are responsible for coordinated the care to people experiencing homelessness that are likely not being captured by CoC, ESG, PATH, RHY or VA resources. These organizations include but are not limited to Federally Qualified Health Centers (FQHC), Hospitals and crisis units; the Public Health Trust (Jackson Health System), the Miami-Dade County Corrections and Rehabilitation social service workers, the Miami-Dade County Juvenile Assessment Center and Juvenile Detention Center, 11th Judicial Circuit; Health Management Organizations, Public Child Welfare Agencies and Managing Entities; and, organizations providing overnight shelter or rental assistance to people experiencing homelessness with philanthropic funding.

All CoC, ESG, PATH and RHY funded agencies are required to participate in HMIS. CoC contracted agencies who operate separate homeless programs that are funded through philanthropic resources will be required to have no less than 85% HMIS participation in homeless programs agency-wide. The Homeless Trust will meet with HMIS project staff on a routine basis to provide training on system changes and capabilities, review utilization reports, discuss issues from end-users or CHOs, and trouble shoot problems with the database system. CHO's will also receive HMIS information via email or through the ServicePoint "System News" feature.

B. Covered Homeless Organization (CHO)

Definition: Any organization (including all its affiliates) that records, uses or processes* PII on clients experiencing homelessness or those at risk of experiencing homelessness for an HMIS (Section 4.1.1, *2004 HMIS Data and Technical Standards*).
*Processing refers to any and all operations performed on the PII (i.e. collection, maintenance, etc.).

Policy: Any agency participating in the CoC HMIS will abide by all policies and procedures outlined in this manual.

Procedure: Any agency, organization or group who has signed an HMIS Agency Agreement with the Homeless Trust will be given access to the Miami-Dade HMIS database. These CHO's will assign a liaison to attend regular HMIS meetings. CHO's may have one or more trained HMIS End Users (see E. HMIS End Users below).

Policy: CHOs are responsible for communicating needs and questions regarding the CoC HMIS directly to the Homeless Trust.

Procedure: HMIS End Users at CHOs will communicate needs, issues and questions to the agency HMIS Liaison. If the CHO is unable to resolve the issue, he/she will contact the Homeless Trust.

C. HMIS End Users

Policy: Any individual who uses ServicePoint must have a signed HMIS End User Agreement on file with the Homeless Trust and abide by all policies and procedures in this

Manual. The CoC HMIS will grant the following permissions to HMIS End Users according to the below hierarchy:
NOTE: These user permission levels are specific to ServicePoint and do not necessarily relate to agency positions.

1. System Administrator
2. Agency Administrator
3. Case Manager
4. Read Only

Procedure:
At each new user training, CHOs are responsible for identifying the employee's role in regard to permissions within the HMIS system.

The CHO's Agency Administrator access level is limited to their agency end users only. An Agency Administrator is responsible for ensuring quality, timely data entry; staying knowledgeable about HUD and CoC regulations as they change; being a point of contact to CoC; notifying the System Administrator of any changes in user access to HMIS, provider address, contact information, or bed count data, if applicable; plus all the responsibilities listed for Case Manager.

A Case Manager is responsible for adhering to policies and procedures in data collection and privacy and security practices, ensuring quality, timely data entry, and correcting errors as they become known. Note: if an Agency Administrator is not assigned the Case Manager will assume the responsibilities of the Agency Administrator until one is assigned. Directors or managers who do not wish to become an HMIS End User but who are ultimately responsible for their agency's HMIS data may attend HMIS trainings as desired and receive aggregate reporting from users they oversee. It is recommended that directors who wish to run reports out of HMIS either become a licensed user (likely an "Agency Administrator") or attend an Advanced Reporting Tool (ART) training and then train staff to forward reports as necessary so that another license is not necessary. Any director or manager who will see any client-level data MUST get an HMIS license and a login.

Individuals from non-HMIS participating agencies, such as those funded by the VA, may request read only access to HMIS for the purposes of service coordination only. Read only licensees are subject to the same training and compliance requirements as all other HMIS End Users. Read only licenses can be assigned at the Case Manager or Agency Administrator level. All requests to access the CoC HMIS are subject to approval by the Homeless Trust. The data collected through HMIS does not require the disclosure of specific diagnosis for disabilities.

D. Services Development Committee

Policy: The Homeless Trust's Services Development Committee will provide community feedback on HMIS implementation related activities and issues.

Procedure: Members of the Services Development Committee (SDC) will invite particularly skilled candidates to join this committee on an as needed basis. The SDC will convene meetings of this group as necessary.

II. Privacy Standards

A. Personally Identifying Information (PII)

Definition: Any information maintained by the Homeless Trust or Covered Homeless Organization about a living homeless client or homeless individual which:

- Identifies, either directly or indirectly, a specific individual;
- Can be manipulated by a reasonably foreseeable method to identify a specific individual; or
- Can be linked with other available information to identify a specific individual (Section 4.1.1, *2004 HMIS Data and Technical Standards*).

Policy: A CHO will enter into the CoC HMIS a required set of data variables for each client, including all universal and program specific data elements, which are specified in the HUD HMIS Data and Technical Standards (see Appendix A for list of Data Elements). The HMIS vendor has implemented electronic mechanisms to corroborate that data has not been altered or destroyed and implemented security measures to ensure PHI is not improperly modified without detection. An audit record of changes is maintained by the HMIS system showing the date and time of any changes recorded, and what end user made the changes. The HMIS vendor only allows sharing of data between authorized HMIS end users.

Procedure: All HMIS End Users will be trained in appropriate and accurate procedures for entering PII into HMIS. This training is provided by Homeless Trust HMIS staff.

B. HMIS Uses and Disclosures

Policy: A CHO may use or disclose PII from an HMIS under the following circumstances:

- To provide or coordinate services to an individual;
- For functions related to payment or reimbursement for services;
- To carry out administrative functions, including but not limited to legal, audit, personnel, oversight and management functions; or
- For creating de-identified PII (Section 4.1.3, *2004 HMIS Data and Technical Standards*).

Procedure: All CHOs must consult the Homeless Trust before providing any information outside of the above stated standards. Disclosure questions should be addressed and documented by Homeless Trust.

C. Applying the Standard

Policy: All standards described in this manual pertain to any homeless assistance organization that records, uses or processes personally identifying information (PII) for an HMIS and/or identify as a CHO. Any CHO covered under HIPAA is not required to comply with the standards in this manual in limited circumstances as defined in the HIPAA rules (Section 4.1.2, *2004 HMIS Data and Technical Standards*).

Procedure: A CHO must comply with HIPAA rules ahead of HMIS policies if it determines that a substantial portion of its PII about homeless clients or homeless individuals is protected health information as defined in the HIPAA rules. The Homeless Trust will exempt HIPAA covered entities from the HMIS privacy and security rules to avoid all possible conflicts between the two sets of rules.

D. Other Allowable Uses and Disclosures

Policy: Provided below are additional uses and disclosures of information allowable by HUD standards. It should be noted that these additional uses and disclosures are permissive and not mandatory (except for first party access to information and any required disclosures for oversight of compliance with HMIS privacy and security standards). However, nothing in this standard modifies an obligation under applicable law to use or disclose personal information (Section 4.1.3, *2004 HMIS Data and Technical Standards*).

Procedure: A CHO must comply with below standards for additional disclosure to applicable entities. All other disclosures must first be approved by Homeless Trust.

1. Legal:

Policy: A CHO may use or disclose PII when required by law to the extent that the disclosure complies with and remains within the boundaries of said law. The following are allowable uses but not a comprehensive list:

- In response to a lawful court order, court-ordered warrant, subpoena or summons issued by a judicial officer, or a grand jury subpoena;
- If the CHO believes in good faith that the PII constitutes evidence of criminal conduct that occurred on its premises

Procedure: A CHO must take immediate actions to notify the Homeless Trust about all legal disclosures. If uncertainty exists about the CHO's authority to disclose, or the action is not specified in this document, the CHO must contact the Homeless Trust Deputy Director before approving any disclosure.

2. Health and Safety

Policy: A CHO may, consistent with applicable law and standards of ethical conduct, use or disclose PII if:

- The CHO, 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
- The use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat.

Procedure: A CHO must take immediate actions to notify the Homeless Trust about all legal disclosures. If uncertainty exists about the CHO's authority to disclose, or the action is not specified in this document, the CHO must contact Homeless Trust administration before approving any disclosure.

3. Abuse, Neglect, Domestic Violence

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

- Where such disclosure is required by law and the disclosure complies and is limited to the confines of said law;
- If the individual agrees to disclosure;
- To the extent that the disclosure is expressly authorized by statute or regulation; and the CHO 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.

Procedure: A CHO that makes a permitted disclosure must promptly inform the individual that a disclosure has been or will be made, except if:

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

4. Law Enforcement

Policy: A CHO may, consistent with applicable law and standards of ethical conduct, disclose PII to a law enforcement official under any of the following circumstances:

- In response to a request for the purpose of identifying or locating a suspect, fugitive, material witness or missing person and the PII disclosed consists only of name, address, date of birth, place of birth, Social Security Number, and distinguishing physical characteristics.

- If the official is an authorized federal official seeking PII for the provision of protective services to the President or other authorized persons OR for the conduct of investigations authorized by 18 U.S.C. 871 and 879 (threats against the President and others).

Procedure: A CHO must take immediate actions to notify the Homeless Trust about all legal disclosures. If uncertainty exists about the CHO's authority to disclose, or the action is not specified in this document, the CHO must contact the Homeless Trust administration before approving any disclosure.

III. Privacy Requirements

Policy: All CHOs must comply with the baseline privacy requirements described here with respect to: data collection limitations; data quality; purpose and use limitations; openness; access and correction; and accountability. A CHO providing emergency shelter to vulnerable persons or residential treatment may adopt procedural privacy protections that exceed the baseline requirements for each of these areas in its privacy notice. A CHO that choses to restrict client visibility by locking the HMIS record may maintain a common data storage medium with another organization (including but not limited to another CHO) that includes the sharing of PII. When PII is shared between organizations, responsibilities for privacy and security may reasonably be allocated between the organizations (Section 4.2, *2004 HMIS Data and Technical Standards)*.

Procedure: All CHO policies regarding privacy requirements must at a minimum include the criteria following in this document. Additional requirements may be added at the discretion of each CHO.

A. Limits on Data Collection

Policy: A CHO may collect PII only when appropriate to the purposes for which the information is obtained or when required by law. A CHO must collect PII by lawful and fair means and, where appropriate, with the knowledge or consent of the individual (Section 4.2.1, *2004 HMIS Data and Technical Standards*).

Procedure: A CHO must post a sign at each intake desk (or comparable location) that explains generally the reasons for collecting any and all information. Data allowable includes all HUD mandated data as well as any other data deemed necessary and approved by the CHO which complies with federal regulations and the policies and procedures of this document.

Additional Privacy Protections

1. Client Confidentiality

Policy: The Homeless Trust HMIS System Administrator and CHOs will ensure the confidentiality of all client data. No identifiable client data will be entered into the CoC HMIS without client consent, and no identifiable client data will be shared outside of the limits of that consent.

Procedure: Access to client data will be tightly controlled using security technology and restrictive access policies. Only individuals authorized to view or edit individual client data will have access to that data.

2. Informed Consent

Policy: CHOs will collect and retain signed client consent forms before any client PII will be entered into the CoC HMIS. CHO staff will thoroughly explain the client consent to each client.

Procedure: Client consent forms must be completed with each individual or household accessing services before any information is entered into the CoC HMIS. Consent forms should be stored in a secure place and maintained by the CHO for seven years.

3. Additional User Privacy Measures

Policy: A CHO may, in its privacy notice, commit itself to additional privacy protections consistent with HMIS requirements, including, but not limited to:

- Restricting collection of personal data, other than required HMIS data elements;
- Collecting PII only with the express knowledge or consent of the individual (unless required by law); and
- Obtaining oral or written consent from the individual for the collection of personal information from the individual or from a third party (Section 4.2.1, *2004 HMIS Data and Technical Standards*).

Procedure: All additional privacy measures must comply with federal regulations and the policies and procedures of this document.

Policy: The CHOs HMIS End Users will be responsible for maintaining updated and accessible privacy notices and other procedures.

Procedure: All user policies must be available to staff members and clients. Changes to privacy notices should be given in advance to all clients and employees using a designated procedure developed by the CHO.

B. Required Data Collection

Policy: CHOs will collect all required sets of data variables for each client as determined by HUD HMIS Data and Technical Standards (see Appendix A for Required Data Elements).

Procedure: Appendix A will contain a listing of data elements to be collected for each client contact in accordance with federal regulations. These data elements may change as HUD HMIS Data and Technical Standards are revised and updated.

C. Appropriate Data Collection

Policy: PII collected by a CHO 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. CoC HMIS End Users will only collect client data relevant to the delivery of services to people experiencing a housing crisis in Ohio Balance of State or surrounding Continuums (Section 4.2.2, *2004 HMIS Data and Technical Standards*).

Procedure: CoC HMIS End Users will refer to policies outlined in the Data Quality Standards for timelines, accuracy and completeness. Users will ask the CHO System HMIS Department for any necessary clarification of appropriate data collection.

D. Privacy Notice -- Identifying Purpose and Use Limitation

Policy: A CHO must use the Homeless Trust-issued privacy notice for the purposes for which it collects HMIS data. A CHO may use or disclose PII only if the use or disclosure is allowed by this standard and is described in its privacy notice (Section 4.2.3, *2004 HMIS Data and Technical Standards*).

Procedure: A CHO may infer its ability to consented use and disclosure of any item 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. A CHO must take immediate actions to notify the Homeless Trust about all legal disclosures.

Additional Uses

Policy: A CHO may, in its privacy notice, commit itself to additional privacy protections consistent with HMIS requirements, including, but not limited to: [How is William tracking ROIs and any additional privacy protections that a CHO may commit to?]

- Seeking either oral or written consent for some or all processing when individual consent for a use, disclosure or other form of processing is appropriate;
- Agreeing to additional restrictions on use or disclosure of an individual's PII at the request of the individual if the request is reasonable. The CHO is bound by the agreement, except if inconsistent with legal requirements;
- Limiting uses and disclosures to those specified in its privacy notice and to other uses and disclosures that are necessary for those specified;
- Committing that PII may not be disclosed directly or indirectly to any government agency (including a contractor or grantee of an agency) for inclusion in any national homeless database that contains personal protected information unless required by statute;
- Committing to maintain an audit trail containing the date, purpose and recipient of some or all disclosures of PII;

- Committing to make audit trails of disclosures available to the homeless individual; and
- Limiting disclosures of PII to the minimum necessary to accomplish the purpose of the disclosure (Section 4.2.3, *2004 HMIS Data and Technical Standards*).

Procedure: Additional privacy protections beyond the baseline requirements are permissible, as exemplified in this policy. Protections should, however, be documented in the privacy notice at all times and approved by Homeless Trust if potentially beyond reasonable scope of authority.

E. Anonymous Clients

Rationale: Anonymous clients in HMIS negatively affect data quality for the Annual Homeless Assessment Report (AHAR) and other HUD reports. HUD does allow for anonymous clients, but they also count that data as missing, and HUD funding is increasingly being tied to data quality. There is certainly a need for Street Outreach to record contacts with clients who need services, but who do not feel comfortable sharing their personally identifying information in HMIS during the engagement phase. Having a clear understanding of the Privacy Policies is a necessity when explaining to clients what purpose their data fills and how it is protected. Based on previous years' data, the CoC HMIS providers have an average of less than 1% of clients not fleeing domestic violence being entered as anonymous.

Policy: The CHO's current year (October 1 to September 30) percentage of anonymous clients not currently fleeing domestic violence shall not exceed 1% of its total clients served during the same period.

Procedure: Refer to the Data Quality Standards for information on how to find the percentage of anonymous clients not currently fleeing domestic violence for a given CHO.

F. Ethical Data

Policy: Data contained in the CoC HMIS will only be used to support the delivery of homeless and housing services in Ohio Balance of State and surrounding continuums. Each HMIS End will affirm the principles of ethical data use and client confidentiality contained in this document.

Procedure: All HMIS CHOs will sign an HMIS Provider Agreement. HMIS End Users will submit an HMIS User Registration Form with an executed HMIS User's Agreement before being given access to the CoC HMIS. Any individual or CHO misusing, or attempting to misuse HMIS data will be denied access to the database, and his/her/its relationship with the CoC HMIS will be terminated.

G. Termination

Policy: All HMIS End Users and CHOs are subject to the privacy and confidentiality terms outlined in this document as well as the federal regulations in the HUD Data and Technical Standards. At any point if a breach of rules and/or policies occurs the user may be penalized by loss of access and/or membership in the CoC HMIS.

Procedure: The CHO or HMIS End User shall inform the System Administrator in a timely manner of any breach to the privacy and security policies outlined in this document, the HUD Data and Technical Standards or security incidents such as suspected or known data breaches. The System Administrator will investigate the issue and determine a proper course of action for correction. If a permanent resolution is unforeseen or the System Administrator deems it necessary, a CHO and/or user termination may occur:

- The Participating Provider will be notified in writing of the intention to terminate their participation in the CoC HMIS.
- The Homeless Trust CoC HMIS System Administrator will revoke access of the HMIS End User or CHO staff.
- The Homeless Trust CoC HMIS System Administrator will keep all termination records on file.

Voluntary Termination

Policy: Should the CHO or HMIS End User decide not to comply with the rules and policies of this document and regulations in the HUD Data and Technical Standards for any reason, they may voluntarily terminate their user agreement with the Homeless Trust.

Procedure: The CHO must use the following measures to terminate participation in the CoC HMIS:

- The CHO or HMIS End User shall inform the Homeless Trust CoC HMIS System Administrator in writing of their intention to terminate their agreement to participate in the CoC HMIS.
- The System Administrator will inform partners and any other relevant parties of the change.
- The System Administrator will revoke access of the CHO and/or HMIS End User in the CoC HMIS.
- The System Administrator will keep all termination records on file.

H. Openness and Disclosures

Policy: A CHO must publish a privacy notice describing its policies and practices for the processing of PII and must provide a copy of its privacy notice to any individual upon request. If a CHO maintains a public web page, the CHO must post the current version of its privacy notice on the web page. A CHO must state in its privacy notice that the policy may be amended at any time and that amendments may affect information obtained by the CHO before the date of the change. (Section 4.2.4, *2004 HMIS Data and Technical Standards*).

Procedure: All amendments to the privacy notice must be consistent with the requirements of these privacy standards. A CHO must maintain permanent documentation of all privacy

notice amendments. Copies of the current privacy notice must be available to all clients, including a sign stating the availability of its privacy notice to any individual who requests a copy. In addition, CHOs who receive federal financial assistance shall provide required information in languages other than English that are common in the community, if speaker of these languages are found in significant numbers and come into frequent contact with the program. *CHOs are also reminded that they are obligated to provide reasonable accommodations for persons with disabilities throughout the data collection process. *Note: This obligation does not apply to CHOs who do not receive federal financial assistance and who are also exempt from the requirements of Title III of the Americans with Disabilities Act because they qualify as ‘‘religious entities” under that Act.

Policy: A CHO may, in its privacy notice, commit itself to additional privacy protections consistent with HMIS requirements, including, but not limited to:

- Giving a copy of its privacy notice to each client on or about the time of first data collection.
- Adopting a policy for changing its privacy notice that includes advance notice of the change, consideration of public comments, and prospective application of changes (Section 4.2.4, *2004 HMIS Data and Technical Standards*).

Procedure: All additional privacy protections must remain consistent with current HUD requirements and be present on the privacy notice.

I. Access and Correction

Policy: A CHO must consider any request by an individual for correction of inaccurate or incomplete PII pertaining to the individual. A CHO is not required to remove any information but may, in the alternative, mark information as inaccurate or incomplete and may supplement it with additional information. A CHO can reject repeated or harassing requests for access or correction (Section 4.2.5, 2004 HMIS Data and Technical Standards).

Procedure: In its privacy notice, a CHO may reserve the ability to rely on the following reasons for denying an individual inspection or copying of the individual’s PII:

- Information compiled in reasonable anticipation of litigation or comparable proceedings;
- Information about another individual (other than a health care or homeless provider);
- Information obtained under a promise of confidentiality (other than a promise from a health care or homeless provider) if disclosure would reveal the source of the information; or
- Information, the disclosure of which would be reasonably likely to endanger the life or physical safety of any individual.

A CHO must document requests for changes to an individual’s PII.

A CHO that denies an individual's request for access or correction must explain the reason for the denial to the individual and must include documentation of the request and the reason for the denial.

Below are the different parties' access levels to data and sharing capabilities. Any additional questions or concerns should be discussed with the System Administrator.

1. Covered Homeless Organization

Policy: CHOs will have access to retrieve any individual and aggregate data entered into the CoC HMIS. When generating reports, users will be able to generate data from any records.

Procedure: The CoC HMIS is a system with shared visibility between HUD, SSVF, and PATH providers. The HMIS Notice of Uses & Disclosures and HMIS Consent to Release and Exchange of Information forms used by the Homeless Trust indicates that the data entered into HMIS is viewable by all users of the system.

2. System Administrator

Policy: The System Administrator will have access to retrieve all data in the CoC HMIS. The System Administrator will not access individual client data for purposes other than maintenance and checking for data integrity. The System Administrator will only report client data in aggregate form.

Procedure: The System Administrator will be responsible for ensuring that no individual client data is retrieved for purposes other than maintenance and performing data quality checks.

3. Client

Policy: Any client will have access on demand to view, or keep a printed copy of, their own records contained in the CoC HMIS. All requests for client information will follow agency policy guidelines for release of information. The client will also have access to a logged audit trail of changes to those records. No client shall have access to another client's records in the CoC HMIS.

*Procedure***:** A client will provide a signed written request to a case manager to see the client's own record. The case manager, or any available staff person within CoC HMIS access, will verify the client's identity and print all requested information. The case manager can also request a logged audit trail of the client's record from the Agency Administrator. The Agency Administrator will contact the System Administrator who will print this audit trail for distribution to the client.

4. Public

Policy: The Homeless Trust staff will address all requests for data from entities other than CHOs or clients. No individual client data will be provided to any group or individual that is

neither the CHO, which entered the data, nor the client without proper authorization or consent.

Procedure: All requests for data from anyone other than a CHO or client will be directed to Homeless Trust staff. As part of the System Administrator's regular employment functions, periodic public reports about homelessness and housing issues in Miami-Dade County will be issued. No PII data will be released in any of these reports.

The Trust will ensure the removal of PHI from any electronic media before the media are made available for reuse. Staff computers are cleared by ITD before reassignment. The Trust documents any record of the movements of hardware and electronic media and any person responsible, and make a retrievable, exact copy of the information shared.

In the event that PHI is shared, as permissible by law, during an emergency or in response to a court order, a record of the data shared will be maintained by the Trust, and the data will be encrypted.

5. Inter-Agency Data Sharing

Policy: All client data entered into the CoC HMIS except Case Notes, Disabling Condition and locked records is viewable by all users.

Procedure: All client acknowledgements of data collection and consent to share data forms used by CHOs must indicate that the data entered into the CoC HMIS is viewable by all users of the system.

6. Access to Core Database

Policy: No one will have direct access to the CoC HMIS database unless explicitly given permission by the Homeless Trust.

Procedure: Under contract with the Homeless Trust, Wellsky will monitor access of the database server and employ security methods to prevent unauthorized database access.

7. On-Site Review

Policy: The Homeless Trust may perform annual on-site reviews at each CHO of data processes related to the CoC HMIS.

*Procedure***:** This review may be done as part of contract monitoring.

J. Accountability

Policy: A CHO must adhere to confidentiality, privacy and security standards. A CHO must establish a procedure for accepting and considering questions or complaints about its privacy and security policies and practices.

Procedure: Each CHO must develop and maintain a written copy of procedures for accepting and considering questions or complaints. This must be accessible to all staff members and updated as needed to comply with all HUD regulations. A CHO must require each member of its staff (including employees, volunteers, affiliates, contractors and associates) to sign a confidentiality agreement that acknowledges receipt of a copy of the privacy notice and that pledges to comply with the privacy notice (Section 4.2.6, 2004 HMIS Data and Technical Standards).

Additional Protections

Policy: A CHO may, in its privacy notice, commit itself to additional privacy protections consistent with HMIS requirements. Additional corrections include but are not limited to:

- Establishing a method, such as an internal audit, for regularly reviewing compliance with its privacy policy;
- Establishing an internal or external appeal process for hearing an appeal of a privacy complaint or an appeal of a denial of access or correction rights; and/or
- Designating a chief privacy officer to supervise implementation of the CHO's privacy standards.

Procedure: Any additional privacy protections should comply with all federal HUD HMIS Data and Technical Standards and policies in this document. Additional protections must be written out in each CHO's policies and procedures documents.

K. Client Grievance

Policy: Clients will contact the CHO with which they have a grievance for resolution of HMIS problems. CHOs will report all HMIS-related client grievances to the Homeless Trust HMIS staff.

Procedure: Clients will bring HMIS complaints directly to the CHO with which they have a grievance. CHOs will provide a copy of the Homeless Trust CoC HMIS Policies and Procedures Manual and Grievance Standards upon request, and respond to client issues.

Policy: If the client is not satisfied with the results of the grievance with the CHO, the client may contact the Homeless Trust for further assistance.

Procedure: Clients bringing HMIS complaints to the Homeless Trust will be subject to the Homeless Trust CoC Grievance Standards.

L. User Grievance

Policy: Users will contact CHO with any grievance regarding HMIS.

Procedure: Users will bring HMIS complaints directly to CHO. CHO will provide a copy of the Homeless Trust CoC HMIS Policies and Procedures Manual upon request, and respond

to any user issues. CHO will send written notice to the Homeless Trust of any HMIS-related user grievance they cannot resolve internally. The Homeless Trust will record all grievances in writing.

IV. Security Standards

A. System Security

Policy: A CHO must apply system security provisions to all the systems where personally identifying information is stored, including, but not limited to, a CHO's networks, desktops, laptops, mainframes and servers (Section 4.3.1, 2004 HMIS Data and Technical Standards).

Procedure: Each CHO must apply and maintain security provisions in the form of virus protection, firewalls, and other provisions listed below in this section to ensure the confidentiality of its clients.

1. Additional Security Protections

*Policy***:** A CHO may commit itself to additional security protections consistent with HMIS requirements by applying system security provisions to all electronic and hard copy information that is not collected specifically for the HMIS. A CHO may also seek an outside organization to perform an internal security audit and certify system security (Section 4.3.1, 2004 HMIS Data and Technical Standards).

Procedure: Additional security protections may be utilized as each CHO believes necessary, but must be compliant with HMIS requirements.

2. Hardware/Software Requirements

Policy: CHOs will provide their own computer and method of connecting to the Internet, and thus the CoC HMIS.

Procedure: It is the responsibility of the CHO to provide a computer and connection to the Internet.

3. Data Access Location

*Policy***:** Users will ensure the confidentiality of client data, following all security policies in this document and adhering to the standards of ethical data use, regardless of the location of the connecting computer. All users are prohibited from accessing the HMIS database from any location other than the designated and approved work site.

Procedure: All Policies and Procedures and security standards will be enforced regardless of the location of the connecting computer. All HMIS related data entry will be processed at

a designated and approved work site. The System Administrator will provide any additional clarification.

4. User Access

Policy: Only authorized users will have access to the CoC HMIS via a user name and password. Users will keep their access information confidential.

Procedure: The System Administrator will provide user names and initial passwords to each user upon completion of training and signing of user agreements and receipt of this Security and Privacy Policies and Procedures document. Written information specifically pertaining to user access (e.g., username and password) may not be stored or displayed in any publicly accessible location. User names will be unique for each user and will not be exchanged with other users. The sharing of username and passwords will be considered a breach of policy resulting in access being revoked. Passwords will be reset every 45 days. Agencies will notify the System Administrator immediately of employee reassignment to non-HMIS job responsibilities or termination so the login can be inactivated. Users not accessing CoC HMIS within three months may have their login inactivated.

5. Virus Protection

Policy: A CHO must protect systems that access HMIS from viruses by using commercially available virus protection software. It may also commit itself to additional security measures beyond this standard if in line with HMIS regulations.

Procedure: A CHO must regularly update virus definitions from the virus software vendor. Virus protection must include automated scanning of files as they are accessed by users on the system where the HMIS application is accessed.

6. Firewalls

Policy: A CHO must protect systems the access HMIS from malicious intrusion behind a secure firewall. It may also commit itself to additional security measures beyond this standard if in line with HMIS regulations.

Procedure: Each CHO must maintain its own up to date firewall, however, each individual workstation does not need its own firewall, as long as there is a firewall between that workstation and any systems, including the Internet and other computer networks, located outside of the organization.

7. User Licenses

Policy: User licenses are controlled by the Homeless Trust regardless of program access. All CHOs participating in the CoC HMIS will receive HMIS access free of participation fees.

Procedure: Licenses are assigned once training is completed successfully.

8. HMIS End User Agreements

Policy: Each HMIS User will sign an HMIS User Agreement before being granted access to the CoC HMIS.

Procedure:
The System Administrator will instruct new users on the process for completing the training after obtaining an HMIS User's Agreement. [Training first before execution of agreement per model end user agreement – also see the revised Trust End User Registration Form?]

Training may be followed by a quiz that tests users on their understanding of the HMIS workflow and privacy and security issues. An original signed copy of the HMIS User's Agreement must be maintained by the CHO. Upon receipt of the agreement by, the user account will be updated to reflect that all requirements have been met.

9. HMIS Agency and Agency Administrator Agreements

Policy: Each agency participating in the CoC HMIS will sign an HMIS Provider Agreement before any data may be entered for its clients.

Procedure: The System Administrator will instruct agencies on the process for completing and submitting the HMIS Provider Agreement.

An original signed copy of the Provider Agreement must be maintained by the Homeless Trust. Upon receipt of the agreements by the Homeless Trust, the provider records will be updated to reflect that all requirements have been met.

10. Training

Policy: All users must be trained by the Homeless Trust and sign an HMIS User Agreement prior to receiving a login to the HMIS.

Procedure: CHO Agency Administrators or Executive Directors can sign up new or current users for HMIS training by emailing homelesstrust@miamidade.gov. Homeless Trust staff will provide training to all new users. Agency Administrators will be given additional training relevant to their position, at least monthly. The System Administrator will provide periodic training updates for all users. The Homeless Trust will be responsible for ensuring that users are instructed in both policies and security.

11. Data Retrieval

Policy: CoC HMIS End Users will maintain the security of any client PII data extracted from the database and stored locally, including all data used in custom reporting. CoC HMIS End Users will not electronically transmit any PII client data across a public network.

Procedure: PII data extracted from the database and stored locally will be stored in a secure location and will not be transmitted outside of the private local area network. Security questions will be addressed to the System Administrator.

B. Hard Copy Security

Policy: A CHO 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 and signed consent forms. CHO may commit itself to additional security protections consistent with HMIS requirements by applying hard copy security provisions to paper and hard copy information that is not collected specifically for the HMIS (Section 4.3.2, 2004 HMIS Data and Technical Standards).

Procedure: A CHO must supervise at all times any paper or other hard copy generated by or for HMIS that contains PII when the hard copy is in a public area. When CHO staff is not present, the information must be secured in areas that are not publicly accessible. Written information specifically pertaining to user access (e.g., username and password) must not be stored or displayed in any publicly accessible location.

C. Physical Access

Policy: A CHO must staff computers stationed in public areas that are used to collect and store HMIS data at all times. When workstations are not in use and staff is not present, steps should be taken to ensure that the computers and data are secure and not usable by unauthorized individuals. A CHO may commit itself to additional security protections consistent with HMIS requirements.

Procedure: A CHO must take steps to secure each computer by automatically turning on a password protected screen saver when the workstation is temporarily not in use. If staff from a CHO will be gone for an extended period of time, staff should log off the data entry system.

1. CHO Technical Support Requirements

Policy: CHOs will provide their own technical support for all hardware and software used to connect to the CoC HMIS.

Procedure: CHOs will provide technical support for the hardware, software and Internet connections necessary to connect to the CoC HMIS according to their own organizational needs.

D. Disaster Recovery

HMIS is a web-based system that is accessible online and is backed up automatically by the HMIS vendor. The vendor has protocols to back up data at a second secure location to allow for use of the system during a disaster. The vendor tests security protocols. The system is accessible from connected mobile devices such as cell phones, tablets and laptops, as well as personal computers. The HMIS vendor has implemented procedures for

allowing access to their facility and/or software in support of data recovery under the disaster recovery and emergency management plan. They have adopted procedures to safeguard facility and equipment from unauthorized access, tampering, and theft. Their procedures include documenting repairs and modifications to physical components of facility related to security.

V. Data Quality

A. Data Entry

Policy: CoC HMIS End Users will be responsible for the accuracy of their data entry.

Procedure: The CHO must maintain standards for periodically checking data for completeness, accuracy and timeliness. The Homeless Trust maintains Data Quality Standards to help all CHOs manage the monitoring of their data quality. The System Administrator will perform regular data quality checks on the CoC HMIS using the Data Quality Standards. Any patterns of error will be reported to the Agency Administrator. When patterns of error have been discovered, users will be required to correct the data, data entry processes (if applicable) and will be monitored for compliance.

B. Data Quality Plan

Policy: The Data Quality Standards, designed by the Homeless Trust in collaboration with the Services Development Committee, is the official document pertaining to all data quality measures including but not limited to accuracy, completeness and timeliness. This should be referenced for all data quality standards. Any questions about materials in this document or items that are unclear should be addressed with the Homeless Trust.

Procedure: The Data Quality Standards should be referenced and followed for all data quality procedures. Each CHO must retain copies of this document and have available for all relevant staff members. If questions are left unaddressed, they should be brought to the attention of the Homeless Trust in a timely manner.

C. New Provider Data

Policy: All new programs, projects or providers are to be entered into the CoC HMIS by the System Administrator.

Procedure: New programs, projects or providers are to contact Homeless Trust HMIS staff to inform of the intent for new information in HMIS. Homeless Trust CoC HMIS staff will verify the project information and then enter the appropriate data into the CoC HMIS.

Policy: All provider data including but not limited to name, project type, bed counts, address, and contact information in HMIS must be kept up to date. New project information will be reviewed by the System Administrator.

Procedure: Any changes to a provider's data should be reported immediately to System Administrator.

Appendix A: Data Elements

Universal

1. Name
2. Social Security Number
3. Date of Birth
4. Race
5. Ethnicity
6. Gender
7. Veteran Status
8. Disabling Condition*
9. Residence Prior to Project Entry
10. Project Entry Date
11. Project Exit Date
12. Destination
13. Personal Identification Number
14. Household Identification Number
15. Relationship to Head of Household
16. Client Location
17. Length of Time Homeless
18. Housing Move in Date

* This UDE will not be visible to all HMIS users. HMIS users must collect this information as part of intake in accordance with Data Quality Standards.

Program-Specific Data Elements

1. Housing Status
2. Income and Sources
3. Non-Cash Benefits
4. Health Insurance
5. Physical Disability
6. Developmental Disability
7. Chronic Health Condition
8. HIV/AIDS
9. Mental Health Problem
10. Substance Abuse
11. Domestic Violence
12. Contact
13. Dates of Engagement and Enrollment
14. Veterans Information

15. Services Provided
16. Financial Assistance Provided
17. Housing Assessment at Exit
18. PATH Status
19. Connection with SOAR
20. BCP Status
21. Sexual Orientation
22. Last Grade Completed
23. School Status
24. General Health Status
25. Employment Status
26. Pregnancy Status
27. Referrals Provided
28. Reason for Leaving
29. Formerly a Ward of Child Welfare / Foster Care Agency
30. Formerly a Ward of Juvenile Justice System
31. Young Person's Critical Issues
32. Referral Source
33. Commercial Sexual Exploitation
34. Commercial Labor Exploitation
35. Transitional, Exit-care, or Aftercare Plans and Actions
36. Project Completion Status
37. Family Reunification Achieved
38. Dental Health Status
39. Mental Health Status
40. Medical Assistance
41. T-Cell (CD4) and Viral Load
42. Percent of AMI
43. Last Permanent Address
44. HP Screening Score
45. VAMC Station Number