PINELLAS CONTINUUM OF CARE

Data and System Performance Committee Meeting
March 21, 2024, 9:00 a.m. – 11:00 a.m.
Allendale United Methodist Church

The Pinellas Continuum of Care is dedicated to ensuring homelessness is a rare, brief, and one-time experience.

Time	Topic/Materials	Action	Lead
9:00 a.m.	Welcome and Introductions	Information	Chair
9:02 a.m.	Approval of March agenda	Action	Chair
9:05 a.m.	Approval of February minutes	Action	Chair
9:10 a.m.	Gold Star Award for February	Action	Chair
9:20 a.m.	First Quarter Data Review - Prevention and rapid rehousing - SPM	Discussion	Chair
10:15 a.m.	HMIS Policies and Procedures, Data Quality Plan, and Data Security Plan	Discussion	Chair, HLA Staff
10:40 a.m.	Open Forum	Discussion	Chair
10:50 a.m.	HMIS Governance Committee	Action	Chair, HLA Staff
11:00 a.m.	Adjourn		Chair

PINELLAS CONTINUUM OF CARE

Data and System Performance Committee
February 15, 2024 | 9:00 a.m. to 11:00 a.m.
Allendale United Methodist and Zoom

In Person Attendees:

Attendees		HLA Staff
Samuel Picard	Lt. Zach Haish	Tony Salgado
Ricky Zanker		Lara Wojahn
Helen Rhymes		

Online Attendees:
Cynthia Kazawitch, Cassie Hefner, Dominique Randall, Christa Bruning, Bryan McCurry, Imani Smith.

Welcomes & Introductions

- The meeting opened at 9:06 AM.
- Quorum established at 9:06 AM using in-person and online committee members.
- Chair Sam Picard asked for introductions from the room as well as those in attendance online.

Approval of Agenda

- Agenda for the February Data and System Performance Committee was sent out electronically for review prior to the meeting.

Motion: Ricky Zanker moved to approve the Agenda. Seconded by Lt. Haish, all in favor, none opposed. Motion passes unanimously.

Approval of Minutes

- Minutes for the January Data and System Performance Committee were sent out electronically for review prior to the meeting.

Motion: In accordance with Roberts' Rules for small meetings, Sam Picard proposed approving the minutes absent any objections. No objections.

Gold Star Award (January)

- The first month using the new process whereby the Gold Star is awarded to different categories of services. This month is for Programs in the OTH Category: which includes Other, Street Outreach, and Homeless Prevention. The rationale for the new approach was revisited and it is so similar programs are competing against each other, and it is a fair comparison.
- HLA staff presented two candidates for the January Gold Star Award: The Florida Dream Center had 99.36% data accuracy and completeness and Boley had 99.06% data accuracy and completeness. HLA recommends Florida Dream Center.
- Sam Picard mentioned that he would like to see in the HMIS newsletter where they interview the winner of the gold star a three-sentence blurb about what the agency does to inform readers about programs to which they have not had prior exposure.

Motion: Lt. Haisch moved to approve the Gold Star Award to Florida Dream Center. Seconded by Helen Rhymes. Unanimously approved.

First Quarter Data Review

- HLA Staff presented the Q1 performance data (October – December 2023) for the CoC. The total client inflow was down 17% from the previous year to 1,155. The total client outflow to permanent housing was up 9% from the prior year to 460. Total clients served was 9,368, down 8% from the prior year.
- The committee discussed the meaning of the data. Lt Haish wondered if there would be value in breaking the entry and exit data down between single individuals and families.
- ACTION ITEM: HLA staff committed to bringing entry and exit data broken down between single individuals and families to the next meeting.
- The group discussed the varying levels of need and services required for different types of clients. Some clients require a much higher intensity of service because they are more vulnerable. The question we need to ask is about who in the system is getting their needs met and who is not being served effectively.
- In the discussion about the Clients Served data, Helen Rhymes noted that there is no consistency between the street outreach teams deployed by the various municipalities.
- The group discussed various situations that would result in clients halting contact with their case managers and not communicating so it is difficult to know whether the demographic not counted here have self-resolved or if they remain homeless. The question then becomes whether it's a lack of prevention funding that is suppressing the exit to permanent housing statistics or if it's because the clients themselves stopped communicating or self-resolved. The group wants to see where the other 45% went that had asked for service.
- Sam Picard asks if it is possible to see whether potential clients who have not been provided prevention services end up going to emergency shelter or receiving other services.
- ACTION ITEM: HLA Staff will look at reason for exit – breakdown the prevention exits.
- ACTION ITEM: HLA Staff will look into bringing the full picture of where clients are going after they ask for help to the committee if they are not a successful prevention client.

CoC System Indicators – SPM Discussion

- HLA Staff mentioned that the SPM data is finally working in HMIS so for the next meeting HLA Staff will bring system performance benchmarks.

PIT and HIC Data

- HLA staff will be sending out emails to request HIC inventory for the night of the PIT.
- Lt. Haisch noted that folks in custody are more likely to reveal a permanent address upon release versus upon arrest. He will have the data by April 26, 2024, after the Sheriff signs off.
- HLA Staff noted that this data isn't going to HUD.
- 380 total volunteers for PIT.
- There was discussion about what some volunteers have done in California where they were trained to count an individual even though they didn't complete the interview. However, this would run the risk of having the individual counted multiple times.
- HLA Staff also noted that HUD will refuse interviews that do not contain demographic data such as race or gender. This will inevitably result in some homeless not being counted because they didn't answer all the questions.

Open Forum

- Lt Haisch would like a breakdown of how many people exit into actual housing via rapid rehousing providers. Do they come from emergency shelter or other originations?
- Helen Rhymes notes that we would have to gather data on what rapid rehousing programs are out there and which ones focus on families versus individuals.
- There was some discussion about which rapid rehousing programs were funded through the most recent HUD NOFO. Many did not receive funding.

- With regard to the emergency shelter data with 0 nights stay, there are folks that do not stay because they can't abide by curfew or some other rule, and there are some folks that are successfully diverted from shelter, so some 0 nights could be a positive result.
- HLA Staff will look into what the prior directive for scrubbing certain stays at the Safe Harbor.
- Sam Picard thinks the Stella P tool will be very helpful to figure out where the system is falling short. Many of the rapid rehousing failures may be a result of a lack of affordable housing and a variety of types of housing. The high acuity clients are higher on the shelter prioritization list, but we could be missing helping some of the other clients.

Action Items

- ACTION ITEM: HLA staff committed to bringing entry and exit data broken down between single individuals and families to the next meeting.
- ACTION ITEM: HLA Staff will look at reason for exit – breakdown the prevention exits.
- ACTION ITEM: HLA Staff will look at bringing the full picture of where clients are going after they ask for help to the committee if are not a successful prevention client.
- ACTION ITEM: HLA Staff will look into what the prior directive for scrubbing certain stays at the Safe Harbor.

March Agenda

- HLA Staff will present more in-depth data for Q1 on prevention and rapid rehousing.
- HMIS Policies and Procedures, Data Quality Plan, and Data Security Plan review

Sam Picard adjourned the meeting at 10:04 am

Pinellas Continuum of Care
Ending Homelessness Together

2024 HMIS P & P Revisions

General Changes and Updates

- Staff titles and grammar changes were made/updated.
- Checked all links and updated when necessary throughout the document for ease of use for the reader.
- Updated WellSky's module name from "ServicePoint" to "Community Services."

HUD HMIS Data and Technical Standards Final Notice – Page 3

- Updated the HUD HMIS Data and Technical Standards Final Notice to include changes made in the HUD HMIS Data Standards Manual Version 1.1.

Domestic Violence Shelters and Programs – Page 3

- Updated "victim" to "survivor" in accordance with HUD's client-focused approach in the 2024 HUD Data Standards.

Policy 1-6: User – User Responsibility – Page 11

- Added the word "completing." The sentence now reads: Attending and completing all required Pinellas HMIS trainings.
- Added the term "data quality." The sentence now reads: Adhering to data entry and data quality requirements.

Policy 1.9 - Required Licensing Fees – Additional Licenses – Page 14

- Added clarification about purchasing additional HMIS licenses during the billing cycle and invoicing.

Policy 2-6: Confidentiality – Page 26

Recommended by Data and System Performance Committee (DSP) for clarity.

- Updated Pinellas HMIS Corrective Action further explains the difference between low, medium, and critical data risks.
- Added a sentence to the preamble to mention Data Quality.
- Added "Security Officer" to the end of the Critical Risk statement.
- Added the statement to Medium Risk that adds another escalation for data quality issues.
- Added a statement to Low Risk to better match what is stated in the Data Quality Plan's proposed changes.
- Added a full statement before the action steps that outlines DSP's involvement in an escalated Data Quality Corrective Action Plan.
- Deleted the statement "aside from data quality certification issues," from the HMIS Governance statement that directly follows the new Data Quality statement.

- Added HMIS Lead to various action steps to bring it more in line with Data Quality instead of exclusively focusing on Data Security.

Policy 2-11: Pinellas HMIS Grievance – Page 33

- Added the HLA Chief Administrative Officer as another level of communication in the grievance procedure.

Policy 4.2 Data Quality Monitoring – Page 47

- Replaced the "Data Completeness report" to the "Data Quality Certification report" for monthly submission by agencies.

Policy 5-1: Technical Support – Page 49

- Under chain of communication added 5. HLA Chief Administrative Officer.

Policy 6-1: Pinellas HMIS Training Descriptions – Page 51

- Replaced "HMIS Advanced Report Training" to "HMIS Intermediate Report Training."
- Updated HMIS Annual Refresher timeline for clarification on when end-users are enrolled into courses and when they are due. End-users offered feedback regarding the submission date and HMIS created a more flexible timeline to complete courses.
    - Used to read that end-users were enrolled in October and courses were due in November.

Pinellas Continuum of Care
Ending Homelessness Together

2024 HMIS Data Quality Plan Revisions

Provider Accountability – Page 6

- Reformatted paragraph into a step-by-step process for clarity
- In step 2, a timeframe of "three months" was added as a determining factor in proceeding with corrective action.
- Moved the section discussing communication from between steps 2 and 3, then placed it at the end of this section.

CoC Data Quality Benchmarks – Page 8

- Replaced previous benchmarks with the updated 2024 Benchmarks.
    - Benchmarks approved by the CoC Board in January 2024.

Pinellas Continuum of Care

Ending Homelessness Together

Homeless Management Information System (Pinellas HMIS)

Policies and Procedures

Table of Contents

OVERVIEW AND INTRODUCTION

These Policies and Procedures were developed to guide the operation of the Pinellas Homeless Management Information System (Pinellas HMIS). The Pinellas HMIS is a tool to help housing and homeless providers track individuals and families who are homeless or at risk of becoming homeless, to assure they have access to housing and supportive services that are appropriate to their housing, health, and human service needs.

The Pinellas HMIS Governance Committee oversees and guides the development and management of the Pinellas HMIS. The Pinellas HMIS Governance Committee is comprised of the Executive Committee of the Homeless Leadership Alliance of Pinellas, Inc. Through the direction of these dedicated members, these Policies and Procedures reflect the community's stance on the operation of the Pinellas HMIS. The Homeless Leadership Alliance of Pinellas, Inc. is the Lead Agency for Pinellas HMIS and convenes the Pinellas HMIS Governance Committee.

The Pinellas HMIS Governance Committee has as guiding principles that the Pinellas HMIS:

- Minimizes risk and maximizes benefits for homeless individuals and families
- Is designed to respect and meet the needs of consumers
- Is a reliable, flexible, and consistent technological system to benefit persons who are homeless or at risk of becoming homeless by providing data that:
    - Captures accurate local and regional information about characteristics and service needs, and
- Prioritizes data security that balances:
    - Confidentiality, so that only authorized people see the data;
    - Integrity, so that data is not modified in any way; and
    - Availability, so that data is accessible to those who use it when they need it.

Clients must give Informed Consent or Release of Information (ROI) to having their data entered into the Pinellas HMIS. They must also authorize the sharing of their data and may specify with whom it may be shared via the ROI. They may decide not to share their data and they may not be denied Member Agency services for lack of participation. However, it will not place the client on the Coordinated Entry list if the information is not entered into Pinellas HMIS.

Pinellas HMIS is also used to inform public policy makers about the extent and nature of homelessness in Pinellas County. The Pinellas Continuum of Care endorses the philosophy of Housing First and believes it will greatly assist in the goal of making homelessness rare, brief, and a one-time experience when data is used to drive decisions. This is accomplished through analysis of data that is grounded in lived experiences of homeless persons and the service providers who assist them in shelters and homeless assistance programs. Information is gathered via consumer interviews conducted by service consumers which is then analyzed. The resulting statistics are used to develop an unduplicated count; aggregated (void of any identifying client level information); and made available to policy makers, service providers, advocates, and consumer representatives. Pinellas HMIS regulates Pinellas HMIS licenses for community stakeholders serving homeless persons, also known as Covered Homeless Organizations (CHO) or Member Agencies (MA). Many MA or CHO's do not receive CoC funding and participate in HMIS voluntarily. All CoC funded, contracted agencies are required to participate in Pinellas HMIS.

The Pinellas HMIS utilizes web-based software from WellSky. Through this software, homeless service organizations across the Continuum of Care (CoC) can capture information about the clients they serve. Pinellas HMIS staff provides technology, training, and technical assistance to users of the system.

BENEFITS OF PINELLAS HMIS

For individuals and families

- Decrease in duplicative intake and assessments
- Streamline referrals
- Case management coordination
- Improved benefit eligibility determination

For case managers

- Use of web-based software to assess clients' needs and to inform clients about services offered on site or available through referral
- Use of on-line resource information to learn about resources that help clients find and keep permanent housing or meet other goals clients have for themselves
- Improve service coordination when information is shared among case management staff within one agency or with staff in other agencies (with written client consent) who are serving the same clients

For agency and program managers

- Improve data used for preparing reports to funding entities, boards, stakeholders and advocacy for additional resources
- Enhance coordination of services, internally among agency programs and externally with other service providers
- Aggregate information that can be used in program design and implementation through a more complete understanding of clients' needs and the ability to track client outcomes
- Capacity to automate the generation of numeric statistics for use in HUD APRs

For community-wide Continuum of Care and policy makers and other advocates

- Understand the extent and scope of homelessness
- Identification of service gaps
- To help address community-wide issues
- Enable McKinney-Vento funded organizations to meet the congressional mandate specified in the HUD Data and Technical Standards Final Notice
- Utilization of aggregated information for system design
- Gather unduplicated count of clients
- Access to aggregate reports
- Utilization of the aggregate data to inform policy decisions aimed at addressing homelessness at local, state and federal levels, in hopes to make homelessness within the CoC rare, brief, and a one-time experience

HANDBOOK FORMAT

This handbook contains the most current information on the operation of the Pinellas HMIS. It is expected that information will be added, removed and altered when necessary and for this reason the Handbook is in modular form so that outdated information may be easily removed and updated information added. For ease-of-use pagination is by Section and Policy Number.

ACKNOWLEDGEMENTS

This Pinellas HMIS Operating Procedures Handbook draws the work of Blue Ridge Homeless Management Information System Steering Committee and the New Hampshire Homeless Management Information System. We thank them for their hard work and generosity in letting us adapt their documentation for our use. *-August, 2017*

HUD HMIS DATA AND TECHNICAL STANDARDS FINAL NOTICE

As per HUD HMIS Data Standards Manual Version 1.1 (2023, June):

> A Homeless Management Information System (HMIS) is the information system designated by a local Continuum of Care (CoC) to comply with the requirements of CoC Program interim rule 24 CFR 578. It is a locally implemented data system used to record and analyze client, service, and housing data for individuals and families who are homeless or at risk of homelessness. The U.S. Department of Housing and Urban Development (HUD) through the Office of Special Needs Assistance Programs (SNAPS) partners with other federal agencies to establish the requirements for HMIS to ensure that there is a comprehensive data response to the congressional mandate to report annually on national homelessness. It is used by all projects that target services to persons experiencing homelessness within SNAPS and the office of HIV-AIDS Housing. It is also used by other federal partners from the U.S. Department of Health and Human Services (HHS) and the U.S. Department of Veterans Affairs (VA) and their respective programs to measure project performance and participate in benchmarking of the national effort to end homelessness. The HMIS Data Standards were first published by HUD in 2004 as the HMIS Data and Technical Standards. The HMIS Data Standards were first published by HUD in 2004 as the HMIS Data and Technical Standards. HUD, in collaboration with its federal partners, has continued to update the HMIS Data Standards regularly thereafter. Each updated document supersedes the previously released HMIS Data Standards. A complete historical archive of previous data standards can be found on the HUD Exchange Data Standards page.

DOMESTIC VIOLENCE SHELTERS AND PROGRAMS

Domestic Violence Shelters and Programs—those nonprofit organizations whose primary mission is to provide services to survivors of domestic violence, dating violence, or stalking-are currently prohibited from entering Protected Personal Information (PPI) into any HMIS.

If an organization's primary mission is other than those listed above, they may participate in the Pinellas HMIS.

Section 1: Contractual Requirements and Role

Policy 1-1: Pinellas HMIS Contract Requirements

The Pinellas County Continuum of Care is a governing body made up of elected officials, community leaders, and local non-profit organizations, who created and implemented a ten-year plan to end homelessness in 2008. As stated in the Pinellas County Continuum of Services plan, Opening Doors of Opportunity: A 10-Year Plan to End Homelessness, on Pg. 10 under the section of Coordination & Partnerships: "Incorporate a system for universal intake, assessment and referral with centralized technology and data systems, such as through the Homeless Management Information System (HMIS)."

The Homeless Leadership Alliance of Pinellas, Inc. (HLA) has been designated as the "Collaborative Applicant" by the Pinellas CoC, and as such is the sole eligible applicant for HUD CoC Planning Grant funds and manages the required HUD process on behalf of the CoC. The HLA has also been designated as the "HMIS Lead Agency" and as such is the sole eligible applicant for HUD CoC HMIS project grant funds, and manages the HMIS as required by HUD, ensuring the CoC is in compliance with all applicable HUD rules and regulations.

The HLA will contract for and administer the following:

- Server based software license (Production and Training Systems)
- User licenses issued
- Training for software implementation
- Annual support agreement
- Disaster Protection and Recovery Support
- System-wide reporting

Member Agencies shall sign a Participation Agreement and agree to comply with the policies and procedures approved by the Pinellas HMIS Governance Committee as well as comply with the stated requirements and will be granted access to the Pinellas HMIS software system after:

- The Participation Agreement (PA) has been signed with the HLA, and
- Member Agencies put into place the stated requirements in the PA.
- Users complete a Level II Background Screening; attend a User Training session; and the agency has completed an onboarding discussion.
    - All Pinellas HMIS users need to complete and pass a Level II background screening, prior to attending his or her first Pinellas HMIS training. Pinellas HMIS must ensure that each Member Agency conduct a Level II background screening for all users in the system. Additionally, the Florida Legislature passed a law, effective August 1, 2010, that places new requirements on persons who work with vulnerable populations; 2011 Florida Statute, Section 435 requires that employees and volunteers who work with vulnerable populations undergo and pass a Level II background screening including fingerprinting prior to beginning work. Pinellas HMIS is a shared client information system, each potential user must have completed and passed a Level II background screening prior to attending their first Pinellas HMIS training.

      By law, the HLA cannot ask for a copy of the results as proof of completion, therefore, each organization must attest to Pinellas HMIS compliance by submitting the background screening date of clearance.

Policy 1-2: Pinellas HMIS Governance Committee

An HMIS Governance Committee, convened by the CoC Data & System Performance Committee (DSP), representing stakeholders in the HMIS project, will advise all project activities. The committee schedule is set by the CoC's HMIS Governance Committee (a current Pinellas HMIS Governance Committee Membership List may be obtained from the Continuum of Care).

Governance Procedures

The Pinellas HMIS Governance Committee serves as the decision-making body and provides advice and support to the Continuum of Care. As a sub-committee of the CoC DSP, the HMIS Governance Committee follows the protocol of the CoC.

The Pinellas HMIS Governance Committee will take actions that ensure adequate privacy protection provisions in project implementation.

The Pinellas HMIS Governance Committee has decision making authority in the following areas:

- Determining the guiding principles that should inform the implementation activities of the Pinellas HMIS, including participating organizations, consumer involvement and service programs;
- Selecting the minimal data elements to be collected by all programs participating in the Pinellas HMIS project;
- Defining criteria, standards, and parameters for the release of aggregate data;
- Recommending the software vendor to the governing organization;
- Recommending priorities to the Continuum of Care for identification of funding streams for the CoC and HMIS.

Policy 1-3: Pinellas HMIS Management

The CEO of the HLA is responsible for oversight of all contractual agreements with funding entities, as recommended by the CoC and the Pinellas HMIS Governance Committee.

Pinellas HMIS Management Procedures:

The HLA is responsible for the day-to-day operation and oversight of the system. Decisions made or actions by the HLA or Pinellas HMIS staff which do not satisfy an interested party, which may be an agency(ies) or a client(s), may be brought before the Pinellas CoC Grievance Committee as grievances for review. The CoC Grievance Committee members shall not have a conflict of interest for the grievance they are adjudicating.

HLA responsibilities for the operation and oversight of the system include:

- Management of technical infrastructure;
- Planning, scheduling, and meeting project objectives;
- Coordinating training and technical assistance including an annual series of training workshops for end users and Agency Administrators;
- Establishing a fee schedule for Pinellas HMIS licenses
- Annual and quarterly reporting to include but not limited to:
  - Longitudinal Systems Analysis (LSA) (replaces AHAR)
  - Homeless Point in Time Count (PIT)
  - Housing Inventory Chart (HIC)
  - System Performance Measures (SPM)
  - HUD Notice of Funding Availability (NOFA) Application; and
- Implementing software enhancements recommended by the Pinellas HMIS Governance Committee.

Client Privacy and Data Security
Client privacy and data security are paramount to a successful and collaborative community information system like the Homeless Management Information System (Pinellas HMIS). The Pinellas HMIS staff spend much time working with our vendor as well as each Pinellas HMIS Member Agency to protect client data and privacy within the network. Pinellas HMIS continues to refine its policies and procedures to protect the confidentiality of client data and strengthen the network. All concerns, complaints and handling of privacy will be handled by the Pinellas HMIS Privacy Officer.

Pinellas HMIS Privacy Officer
HLA has assigned a Privacy Officer for Pinellas HMIS who will outline network risk, monitor client privacy in the system, work on policy and procedure creation to protect client data, work with the Pinellas HMIS trainer to improve privacy trainings, and field complaints regarding Privacy and Security violations. The Pinellas HMIS Privacy Officer is the HMIS Trainer Training & Support Coordinator. All concerns about privacy should be sent to https://pinellashmis.zendesk.com/hc/en-us.

Pinellas HMIS Data Security Officer
HLA has assigned a Data Security Officer for Pinellas HMIS who will monitor system and data security, work to improve security within the network members, and work with the Pinellas HMIS trainer to strengthen training around system and data security. All concerns about privacy should be sent to https://pinellashmis.zendesk.com/hc/en-us.

Policy 1-4: Member Agency Responsibility

Each Member Agency will be responsible for oversight of all agency staff that generate or have access to client-level data stored in the system software to ensure adherence to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), HUD Department of Housing and Urban Development Docket No. FR-4848-N-02: Homeless Management Information Systems (HMIS); Data and Technical Standards Final Notice and all State and Federal regulations as well as to ensure adherence to the Pinellas HMIS principles, policies and procedures outlined in this document.

Member Agency Responsibility Procedures

The Member Agency:

- Holds final responsibility for the adherence of the agency's personnel to the HIPAA, HUD Department of Housing and Urban Development Docket No. FR-4848-N-02 Homeless Management Information Systems (HMIS); Data and Technical Standards Final Notice and all State and Federal regulations as well as ensuring adherence to the Pinellas HMIS principles, policies and procedures outlined in this document;
- Is responsible for all activity associated with agency staff access and use of the Pinellas HMIS data system;
- Is responsible for establishing and monitoring agency procedures that meet the criteria for access to the Pinellas HMIS System, as detailed in the policies and procedures outlined in this document;
- Will put in place policies and procedures to prevent any misuse of the database system by designated staff;
- Ensures Pinellas HMIS bed inventory be maintained in real-time: **All Housing Providers** are required to maintain a current bed inventory and notify Pinellas HMIS staff five (5) business days in advance of a change to any beds at the facility; Pinellas HMIS will maintain the bed inventory within Pinellas HMIS
- Agrees to allow access to the Pinellas HMIS System only to staff who have completed and passed a Security Awareness Training, HIPAA Training, Level II Background Screening, and been trained in the Pinellas HMIS system and who have a need for access. Need exists only for those shelter staff, volunteers, or designated personnel who work directly with (or who supervise staff who work directly with) clients or have data entry or technical responsibilities.

The Member Agency oversees the implementation of internal data security policies and standards and :

- Assumes responsibility for integrity and protection of client-level data entered into the Pinellas HMIS system;
- Ensures organizational adherence to the Pinellas HMIS Policies and Procedures;
- Communicates control and data protection requirements to Agency Administrators and users;
- Authorizes data access to agency staff and assign responsibility of the data;
- Monitors compliance and periodically review control decisions;
- Ensures that data is collected in a way that respects the dignity of the participants;
- Ensures that all data collected must be relevant to the purpose for which it is used that the data is entered accurately and on time;
- Provides prompt and timely communications of new programs or project to be added or deleted, data issues, changes in license assignments and user accounts, and software to the Pinellas HMIS HelpDesk; and
- Immediately notifies immediately the Pinellas HMIS System Administrator of any issue relating to system security or client confidentiality.

Policy 1-5: Member Agency Pinellas HMIS Agency Administrator

Every Member Agency shall designate one person to be the Agency Administrator who holds responsibility for the coordination of the system software in the agency. The Agency Administrator role is to act as the liaison between the partner agency and Pinellas HMIS staff. Agency Administrators ensure compliance with HMIS policies within their agency and provide support for HMIS use within their agency, including planning for HMIS knowledge transfer prior to staff's departure from the agency. The Agency Administrator manages data collection and data quality as outlined in the Data Quality Plan.

Pinellas HMIS Agency Administrator Procedures

A successful Agency Administrator possesses the following skills**:**

- Must be computer literate.
- Thorough knowledge of ServicePoint and training can be requested in the event that the Agency Administrator is not familiar with ServicePoint.
- Knowledgeable about the agency's programs and their respective grants.
- Knowledgeable about HUD regulations and reporting requirements across the agency's programs.
- Ability to coordinate multiple projects and meet deadlines.
- Compliance with HUD and local governing agency/entity regulations and standards.
- Should have at least intermediate Excel skills (such as filtering, formatting, simple equations, etc.)

The Agency Administrator will be responsible for duties including:

- Editing and updating Member Agency information;
- Immediately notifying Pinellas HMIS of any new funding, report requirements, and/or projects that need to be built into HMIS. Agency Administrators must submit a Pinellas HMIS Project Setup Form to the Pinellas HMIS Help Desk for each new program;
- Ensuring that access to the Pinellas HMIS is requested for authorized staff members only after:
  a) Confirming the agency's license count. If additional licenses are needed, the Agency Administrator will submit a license request to the Pinellas HMIS Help Desk.
  b) Submitting all completed new end user paperwork. Important fields include the permission level, level 2 background clearance date, primary provider and other programs the end user enters data for, as well as Agency Administrator and end user signature(s).
- Immediately notifying the Pinellas HMIS Help Desk of any HMIS end-users who should no longer have access to HMIS, whether due to changing job responsibilities or departure from the agency;
- Serving as point-person in communicating with Pinellas HMIS staff for data cleanup, training requests, additional license requests, report questions, etc.;
- Facilitating timely reporting from the Member Agency that they represent (unless the Member Agency has designated another person for this function);
- Working cooperatively with Pinellas HMIS staff including checking and responding to data cleanup and data confirmation requests from Pinellas HMIS staff members in a timely manner;

- Attending no less than three quarterly Pinellas HMIS Agency Administrator Meetings held by Pinellas HMIS annually
    - If the Agency Administrator is unable to attend a meeting, they must send an alternate that is registered as Agency Administrator back up with Pinellas HMIS
- Ensure that the most current HMIS Privacy Notice is posted in a visible area and/or verbally communicated with the client in the event of an emergency preventing face-to-face contact in a language that is understood by clients;
- Enforce data collection, entry, and quality standards ensuring completeness, timeliness, and integrity of data following the guidelines in the Data Quality Plan by regularly running data quality reports using the reporting tools located in ServicePoint;
- Correct data quality issues as soon as possible and report unresolved issues to the Pinellas HMIS Help Desk; and
- Provide the monthly Data Quality & Certification form and required documentation on or prior to the due dates listed on the Pinellas HMIS calendar.

The Agency Administrator is also responsible for the implementation of Data Security Policy and Standards, including:

- Following the Pinellas HMIS Security and Privacy Plans;
- Administering agency specified business and data protection controls;
- Administering and monitoring access control;
- Providing assistance in and/or coordinating the recovery of data, when necessary;
- Detecting and responding to violations of the Policies and Procedures or agency procedures; and
- Completing DCF's Security Awareness and HIPAA Basics training and send HMIS their certificates annually.

The HMIS Staff will coordinate training and technical assistance for Agency Administrators.

Agency Administrators not in compliance with the Member Agency Administrator policy and procedures risk having their Pinellas HMIS access suspended. Suspended licenses will not be re-activated until Agency Administrators review all materials pertaining to the specific suspension on the Pinellas HMIS Help Desk.

Policy 1-6: User

All individuals at the Member Agency levels who require access to Pinellas HMIS will be granted such access after training and agency authorization. Individuals with specific authorization can access the system software application for the purpose of conducting data management tasks associated with their area of responsibility.

User Procedures

The Pinellas HMIS Staff authorizes the use of the Pinellas HMIS to users who have received appropriate training, and who need access to the system for technical administration of the system, data analysis and report generation, or other essential activity associated with carrying out Pinellas HMIS responsibilities.

The Member Agency authorizes the use of the Pinellas HMIS only to users who need access to the system for data entry, editing of client records, viewing of client records, administration or other essential activity associated with carrying out Member Agency responsibilities:

User Responsibility

Every Pinellas HMIS End User is responsible for the following:

- Adhering to all of the policy and procedures outlined in this document.
- Attending and completing all required Pinellas HMIS trainings.
- Entering quality data in a timely and accurate manner.
- Adhering to data entry and data quality requirements.

Users are any persons who were trained and have an active license in Pinellas HMIS. They must be aware of the data's sensitivity and take appropriate measures to prevent unauthorized disclosure. Users are responsible for protecting institutional information to which they have access and for reporting security violations. Users must comply with the data security policy and standards as described and stated by the agency and HUD baseline requirements stated in the Final Notice Docket No. FR-4848-N-02. Users are accountable for their actions and for any actions undertaken with their usernames and passwords. Users must advise the Agency Administrator and the Pinellas HMIS System Administrator if their passwords are compromised.

Contractors, volunteers, interns and others who function as staff, whether paid or not, are bound by the same User responsibilities and rules set forth in this manual.

Policy 1-7: Training

Pinellas HMIS staff will coordinate ongoing training schedules for Agency Administrators and Users. The schedule of trainings will be determined on an as-needed basis. All users can request a training by contacting Pinellas HMIS at https://pinellashmis.zendesk.com/access/unauthenticated.

Pinellas HMIS Trainings Offered
Overview of the Pinellas HMIS User:

- Basic: Introduction to the Pinellas HMIS System (End User Training)
- Introduction to the Pinellas HMIS Member Agency Project workflow
- Review of applicable policies and procedures
- Logging on to the Pinellas HMIS System
- Entering client information including demographics, placements and services, HUD data and case management

Program Management Training
Overview of the Pinellas HMIS Project (Agency Administrator):

- Review of Member Agency technical infrastructure including roles and responsibilities
- Review of security policies and procedures
- Overview of Pinellas HMIS agency administrative functions
- Entering and updating information pertaining to the Member Agency
- Review of Pinellas HMIS technical infrastructure
- Reporting with the Pinellas HMIS
    - Introduction to reports
    - Using existing reports
    - Creating new reports
    - Exporting information to other software applications (i.e. Excel and PDF)

Pinellas HMIS Training Process
All end-users are required to have basic computer competency prior to attending any Pinellas HMIS training. End-users should be able to turn on/off a computer, use a mouse and keyboard, launch a browser, enter a URL, and navigate the World Wide Web. End-users who cannot complete these tasks should be sent to a basic computer competency prior to be scheduled for Pinellas HMIS training.

Pinellas HMIS staff will schedule individual training follow-up sessions with each user after the initial training. Failure to attend this follow-up four weeks after the initial follow-up date will result in a profile deactivation until the follow-up is completed. Follow-up to training is done on a one-on-one basis post training to allow for a personalized follow-up, additional assistance, and feedback.

Each HMIS user is required to complete an annual refresher training; HIPAA; and Security Awareness Training; Pinellas HMIS Privacy & Security; and HMIS Data Entry courses; reminders will be sent by Pinellas HMIS staff at least 30 days prior to expiration date. Failure to complete the refresher trainings will result in an inactive license status until the trainings are completed.

Policy 1-8: Amending Pinellas HMIS Policies and Procedures Policy

The HLA reserves the right to change privacy practices and the terms of the Pinellas HMIS Policies and Procedures at any time, including protected personal information (PPI) created or received before the amendment(s), provided such changes are permitted by applicable law.

Amending Procedures

- The CoC's HMIS Data and System Performance Committee is responsible for reviewing these policies and procedures annually. Suggested amendments from this committee will be forwarded to the Pinellas HMIS Governance Committee.
- The Pinellas HMIS Governance Committee is responsible for reviewing and approving these policies and procedures annually.
- Prior to the Pinellas HMIS Policies and Procedures being approved by the CoC Board of Directors, feedback is sought from both the Funder's and Provider's Councils.
- Revisions to any Pinellas HMIS-related policy will be noted as revisions with an effective date.
- Final approval of these Policies and Procedures are approved annually by the CoC Board of Directors at their May board meeting.
- The Pinellas policy and procedures are made available on the Pinellas HMIS HelpDesk at https://pinellashmis.zendesk.com/hc/en-us. Previous editions will be maintained electronically and provided upon request.

Policy 1-9: Required Licensing Fees

Pinellas HMIS staff will monitor and review all user licenses, license usage, and set licensing fees for the Pinellas HMIS annually.

HMIS license costs are often an allowable expense for many federal and local grants that require data entry into an HMIS. Check with your funder or contract to confirm if this is an eligible expense for your agency.

Licensing Fee Procedures

The Pinellas HMIS shall evaluate licensing fees annually and discuss proposed changes with local funding entities. Any price changes for Pinellas HMIS Member Agencies will take effect during the next annual billing cycle, which begins October 1st. The deadline to pay invoices will be 30 days following the invoice date. Any revisions to agency license pools need to be made by the agency administrator before October 1st.

Each HMIS Member Agency is required to pay any associated fees listed below for licenses requested. The fees listed below are non-negotiable.

Unsubsidized License Fees

Item	Description	Fee
New License	There is a vendor one-time setup fee ($145.50) for new licenses and the annual license vendor fee ($254.50). This includes an advanced reporting license. Fees are per new license.	*$400/license**
Annual License Renewal	There is an annual vendor license fee ($254.50). This includes an advanced reporting license. Fees are per license.	*$254.50/license**
Administrative Fee	All licenses will include an additional annual admin fee of $50 per license.	*$50/license**

Fees are subject to change based on vendor pricing changes.

Subsidized License Fees

Subsidized licenses are paid for by grants received by the HMIS Lead and are made available for agencies to participate in HMIS. Agencies who are granted the use of subsidized licenses are responsible for paying the administrative fee per license.

Item	Description	Fee
Administrative Fee	Subsidized licenses (Policy 1-10) also incur an annual admin fee of $50 per license.	*$50/license**

Additional Licenses

If Member Agencies need additional HMIS licenses, the Member Agency Administrator can make a request for additional non-subsidized licenses through the HLA Pinellas HMIS Help Desk (https://pinellashmis.zendesk.com/access/unauthenticated). If a non-subsidized license is purchased after the annual billing cycle begins (October 1st), then the license fee will be prorated and an invoice will be generated for payment. Licenses will be provided to the agency once payment has been processed.

Policy 1-10: Subsidized Licenses

HMIS Member Agencies may be eligible to use subsidized licenses when available. Subsidized licenses waive the New License fees and/or the Annual License Renewal fees; however the Administrative Fee (as outlined n Policy 1-9 above) is applicable to all HMIS licenses and paid for by the Member Agency using the license.

Subsidized License Objective
If subsidized licenses are available, a qualifying HMIS Member Agency may receive up to three (3) subsidized licenses. Subsidized licenses are granted upon a case-by-case basis, subject to availability. Appeals will be reviewed by the HMIS Governance Committee.

Eligibility

New HMIS Member Agencies and existing HMIS Member Agencies that are starting new projects may be eligible for subsidized licenses for those projects if the project meets the following criteria: *the Project has data that fulfills a specific CoC need (i.e., diversion/prevention, target population, missing geographic region, etc.); the Agency has a primary organizational mission to end homelessness; the Project has a primary organizational mission of serving those defined by HUD as Category 1 – Literally Homeless; or the Project is required to enter data into HMIS by a funding entity.*

The types of projects that are prioritized for subsidized licenses may change based on changing CoC needs, changes in funding used by Pinellas HMIS to purchase subsidized licenses, and other factors. Projects whose data is included in HUD reports and local prioritization receive priority consideration. This includes

- **Homeless Diversion/Prevention** - financial assistance and case management providers who help at-risk and homeless individuals and families (defined by the HEARTH Act) remain out of the homeless system of care, retain housing, or quickly exit homelessness to permanent housing.
- **Housing/Shelter** - homeless emergency shelters, transitional housing, or permanent supportive housing whose data are included on the Housing Inventory Count (HIC).
- **Homeless Street Outreach** - teams who contact and engage with homeless clients on the street, places not meant for habitation, or other homeless locations.

New Pinellas HMIS Member Agencies will be assessed for licensing fees prior to gaining access to Pinellas HMIS. Existing Member Agencies will be assessed for licensing fees when new licenses are requested.

Member Agencies who are currently receiving subsidized licenses and no longer meet the criteria for receiving subsidized licenses (eligible projects ending, mission change, service changes, etc.) will be notified via email prior to the new contract year and an invoice for payment of existing licenses will be sent in the new contract year for the Annual Renewal cost. Licenses will not be allocated, and staff training will not be scheduled until payment is received by HLA.

Policy 1-11: Custom Reporting and Custom Assessment Work

Pinellas HMIS software is packaged with a range of standard HMIS reports, data elements, and assessments. Pinellas HMIS staff are equipped to help identify the appropriate resources for HMIS Member Agencies. If the existing resources do not meet a Pinellas HMIS Member Agency's need, Pinellas HMIS Member Agencies are able to request Custom Reports and Custom Assessments be created for them by the Pinellas HMIS System Administrator, Data Analyst, or other Pinellas HMIS staff.

Depending on the scope of work, these requests may be accepted or declined by Pinellas HMIS staff or referred to the Pinellas HMIS vendor. Requests that fall within the normal scope of Pinellas HMIS duties do not incur any additional fees. Requests beyond normal scope, or requests referred to the HMIS vendor, do incur fees as outlined below.

Custom Report and Assessment Fee Schedule

Data Analyst or System Administrator Custom Reporting	There is a fee of $25 per hour for support from either the Data Analyst or Pinellas HMIS System Administrator to create any new reports or customization to an assessment or workflow that goes beyond the normal scope of HMIS duties.	$25/hour for Pinellas HMIS System Administrator (minimum of 2 hours)*
Data Analyst or System Administrator Custom Assessments or Workflows	There is a fee of $25 per hour for support from either the Data Analyst or Pinellas HMIS System Administrator to create any customized assessments or workflows that go beyond the normal scope of HMIS duties.	$25/hour for Pinellas HMIS System Administrator (minimum of 2 hours)*
Vendor Assisted Reports, System Changes, or Technical Assistance	In the event the Pinellas HMIS System Administrator is unable to create a report it will be escalated to the vendor at their rate of $125 an hour. Fees are per report at the current HMIS or vendor rate. Rates subject to change without notice. Will require upfront deposit to spec out report. Upfront deposit goes towards balance of report project.	$125/hour** Vendor

**** Two-hour minimum includes planning, creation, testing, and quality assurance***
***** Fees are subject to change based on vendor pricing changes***

What is considered normal scope for assessments?
HMIS Member Agencies are encouraged to align their data collection needs with the data currently collected, or available, in HMIS to improve the sharing of data between agencies and reduce system bloat caused by having multiple versions of the same data element.
If the assessments and data elements needed, or the scope of data needed, requires significant custom assessment work beyond what is currently available in Pinellas HMIS, the work will be beyond normal scope and will incur the fee, or fees listed above.

Below are characteristics of custom assessment work that goes beyond normal scope and incurs the applicable fee.

- Creating Agency-specific assessments that require the creation of ten or more new assessment questions or five or more sub-assessments.
- Creating custom workflow beyond the standard Entry/Exit or Service workflows where HMIS staff must determine when and how to collect data for agency requests.

What is considered normal scope for custom reports?
HMIS Member Agencies are encouraged to make use of the existing Provider Reports, local Custom Reports, and HMIS Vendor Reports that are made available. However, due to the range of local reporting needs and funder requirements, existing reports may not provide the needed information. In this instance, HMIS Member Agencies are encouraged to request reports from the Data Analyst or Pinellas HMIS System Administrator.

If the report is considered within normal scope by Pinellas HMIS staff, based on the criteria below, the report will incur no charge. However, reports determined to be beyond the normal scope will incur the applicable charges. Beyond normal scope is

Below are characteristics of reports that go beyond normal scope and incur the applicable fee.

- Reports that require the use of more than one visualization and extensive formatting to present data to an audience.
- Reports that require the use of one or more complex calculations.
    - Complex calculations are those that require the use of multiple Queries in SAP Business Objects (also known as ART) and include, but are not limited to, Newly Identified as Homeless, Returns to Homelessness, and Changes in Income, Non-Cash Benefits, or Health Insurance.
- Reports that require the use of more than ten simple calculations.
    - A simple calculation requires the creation of custom objects (Dimensions, Measures, or Details) within SAP Business Objects (also known as ART). This includes, but is not limited to, Length or Enrollment/Stay, Chronically Homeless, Household Type, and any Counts.

Agencies that submit multiple report requests may also incur fees for reporting needs beyond the normal scope. Agencies are allowed to request two (2) basic reports per Fiscal Year (October 1 to September 30). To account for the Agencies that may have additional basic reporting needs due to having additional HMIS projects, agencies are allowed to request an additional report for every ten projects that are actively entering data into Pinellas HMIS to a maximum annual number of 6 basic reports.

A project is considered to be actively entering data if clients are currently enrolled in the project or if clients have received services, recorded in HMIS, in the past 30 days**.**

Number of Active HMIS Projects for the Agency	Number of Basic Reports per Fiscal Year
0-9	2
10-19	3
20-29	4
30-39	5
40+	6

Please note: requesting updates or additions to existing custom reports may count as beyond the normal scope or as an additional report request depending on the frequency and complexity of the request.

Section 2: Participation Requirements

Policy 2-1: HMIS Participation and Implementation Requirements

All prospective health and human service providers who join Pinellas HMIS must sign and agree to abide by the terms of all agency and user-related Pinellas HMIS forms, registration forms, and all policies and procedures.

Participation Requirements
Any 501(c)3 organization that provides a health and/or human service may qualify to participate in Pinellas HMIS. To participate in Pinellas HMIS Member Agencies must sign and agree to abide by the terms of all agency and user related Pinellas HMIS forms and policies and procedures outlined in this document. Participation is voluntary, but strongly encouraged. A fee may be assessed per user to access and enter data into Pinellas HMIS.

- Any 501(c)3 organization whose primary mission involves solving homelessness is strongly encouraged to actively enter data in the Pinellas HMIS.
- All Member Agencies which receive funding from the United States Housing and Urban Development Department (HUD) are mandated to participate in Pinellas HMIS by contract with HUD. Additionally, all Member Agencies which receive funding from the HLA, a local municipality or Pinellas County Government are required participate in Pinellas HMIS as outlined in their contract.

- A service provider whose primary mission is not homeless related, but who provides a basic need, prevention, diversion, or wrap around service is strongly encouraged to actively enter data in the Pinellas HMIS.

Pinellas HMIS Participation Agreement Procedures
COC Membership: Prior to becoming a Pinellas HMIS Member Agency, a prospective Member Agency must first become a member of the Pinellas County Continuum of Care (https://www.pinellashomeless.org/pinellascoc).

New Agency Request: Members of the Pinellas County Continuum of Care interested in becoming a Pinellas HMIS Member Agency must submit a request via the Help Desk to schedule and participate in an onboarding discussion (https://pinellashmis.zendesk.com/hc/en-us/articles/16786220971027-New-Agencies-Interested-in-Entering-Data-in-Pinellas-HMIS-).

Pinellas HMIS New Project Request Form: Prospective Pinellas HMIS Member Agencies should complete the online New Project Request Form for each project the agency intends to enter in Pinellas HMIS. Existing Pinellas HMIS Member Agencies will also need to complete this form to request additional projects be added for their use in Pinellas HMIS (https://pinellashmis.zendesk.com/hc/en-us/articles/16785113003667-Need-a-New-Project-in-HMIS-Use-the-Form-Linked-in-this-Article).

New Member Agency Meeting: Prior to signing any agreements for participation, a prospective Pinellas HMIS Member Agency must participate in an initial onboarding meeting. This meeting can be scheduled via the Help Desk (https://pinellashmis.zendesk.com/hc/en-us/requests/new).

Participants in this meeting should be the Pinellas HMIS staff, the prospective Pinellas HMIS Member Agency CEO/Executive Director or designee, and other Member Agency critical staff; which may include data entry staff, supervisors, managers, intake workers, case managers, or any staff they feel is necessary regarding Pinellas HMIS data entry, data quality, or the reporting process.

The goal of the meeting is to review the submitted Pinellas HMIS New Project Request Form(s); the required data elements; Pinellas HMIS Policy and Procedures; define entry requirements; and set Member Agency expectations. The onboarding meeting will also allow Pinellas HMIS staff to properly assess the prospective Pinellas HMIS Member Agency's workflow, user needs, specific implementation issues, and any constraints or risks that will need to be mitigated by the prospective Pinellas HMIS Member Agency prior to receiving access.

After the onboarding meeting, the prospective member Agency may need to submit additional Pinellas HMIS New Project Request Forms. This form is also to be completed by existing Pinellas HMIS Member Agencies when it is necessary for them to request additional projects be added to Pinellas HMIS.

Identification of a Member Agency Administrator: All Pinellas HMIS Member Agencies shall designate one person to be the Agency Administrator who holds responsibility for the coordination of the system database in the agency. For Member Agencies with more than five employees and licensed Pinellas HMIS users, the Member Agency must assign both an Agency Administrator and a back-up Agency Administrator to coordinate Pinellas HMIS activities for their organization. Agency Administrator role and responsibilities can be found in Policy 1-5.

Security Assessment: Organizations new to the Pinellas HMIS system will need to attend a meeting which would include the Agency CEO/Executive Director or designee, Program Manager/Administrator (if applicable) and Agency Administrator with Pinellas HMIS staff member to assess and complete Agency Information Security Protocols. Agency IT staff may be asked to participate as necessary.

Additionally, the privacy and confidentiality of client information in Pinellas HMIS is essential. It is the Member Agency's responsibility to ensure that personnel complete a Level II Background Screening on all end users. Pinellas HMIS access will not be granted for any individual who has entered a plea of *nolo contendere* (no contest); or been found guilty of any fraud (including identity theft or computer related crimes); or stalking-related felony crimes punishable by imprisonment of one year or more in any state. HLA, as the Pinellas HMIS Lead Agency, is not allowed to view Member Agency personnel's Level II Background Screenings therefore a date of clearance is requested and noted upon submission of the Pinellas HMIS User Permission Request form. Member Agency must complete an annual security review to ensure the implementation of the security requirements for the Pinellas HMIS.

Training: The Member Agency Administrator and designated Pinellas HMIS users are required to attend training(s) prior to accessing HMIS. All Pinellas HMIS user paperwork must be completed in its entirety and signed by the Member Agency CEO/Executive Director or Agency Administrator prior to Member Agency staff attending any trainings.

Client Data: Member Agencies must secure written permission from the client to enter the client's data into the Pinellas HMIS by securing signed Informed Consent or Release of Information from the client allowing permission to share personal information with other member agencies. Data is also collected and shared when verbal consent is obtained—specifically in the case of the Diversion Teams, the Street Outreach and 211 Homeless Helpline. In the event of a declared emergency, verbal consents can be obtained from clients for all partner agencies with the approval of the Continuum of Care (CoC). The most current Privacy Notice can be found on the Pinellas HMIS Help Desk.

Member Agencies will provide written explanation to each client of how information is to be used and stored and on the client's recourse if s/he feels data is misused, e.g., grievance policy. Any incident regarding compromise of client confidentiality must be reported to the Pinellas HMIS staff immediately.

HMIS Signage: The HUD Data and Technical Standard requires as a baseline requirement that every Member Agency post the **Privacy Notice** at each intake desk (or comparable location) that explains generally the reasons for collecting protected personal information (PPI). In the event of a declared emergency, the Privacy Notice can be verbally communicated in a language that is understood by the client when face-to-face contact is not possible. Protected Personal Information (PPI) is defined by HUD as "Any information maintained by or for a Covered Homeless Organization about a living homeless client or homeless individual 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."

Death, Disaster, Public Health Emergencies, or Public Safety: Data within Pinellas HMIS may be used to assist officials during times of death, disaster, public health emergencies, or public safety where clients are at risk. During these instances, the Pinellas HMIS staff will work closely with organizations, public officials, funders, and/or law enforcement to assist clients who are at risk. The Pinellas HMIS staff will only validate information presented to the staff and provide local contact information for the service provider(s) that were in direct contact during a particular service date(s).

Pinellas HMIS staff will not print off, give an electronic copy of, or disclose any other personal information without a subpoena. However, in cases of death, Pinellas HMIS will disclose any next of kin information in the system in addition to provide local contact information for the most recent service provider serving the client.

Policy 2-2: Data Security Responsibility

The HLA will manage the contractual relationship with a third-party software development corporation who will in turn continue to develop, implement and maintain all components of operations of the web-based system including a data security program.

Data Security Procedures

The Pinellas HMIS Governance Committee will:

- Define the data security program;
- Implement its standards; and
- Promote awareness of the program to all interested parties.

Access to areas containing Pinellas HMIS material, equipment, data, and software will be secured. All client-identifying information will be strictly safeguarded in accordance with appropriate technical safeguards. All data will be securely protected to the maximum extent possible.

The scope of security includes:

- Technical safeguards;
- Physical safeguards, including, but not limited to locked doors;
- Network protocols and encryption standards such as https/ssl encryption (an indicator of encryption use) and client data security (Data Encryption);
- The use of system auditing tools to ensure system oversight, investigate privacy or security breaches, and filed client grievances; and
- Server and client-side certificates.

Pursuant to 42 and 45 CFR notwithstanding, Pinellas HMIS is an open or shared HMIS system. The default visibility settings for clients will be set to OPEN for all Pinellas HMIS clients that are not registered or receiving services from any 42 or 45 CFR facility or program. If a client is enrolled in a 42 or 45 CFR covered entity program, the Member Agency Administrator will notify Pinellas HMIS of program visibility settings which will be set in accordance to applicable laws.

Member Agencies are responsible for:

- Ensuring virus protection is updated
- Maintain a system firewall
- Protect physical access to computers with access to Pinellas HMIS data

Policy 2-5: Client Consent for Electronic Data Sharing

All Pinellas HMIS users will adhere to the basic business practices under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) as it relates to client confidentiality, privacy, and security.

Informed Consent and Release of Information
Pinellas HMIS requires a client's signature on the Pinellas HMIS Informed Consent and Release of Information or provide verbal consent prior to their information being entered into Pinellas HMIS. Informed consent must be based upon a clear appreciation and understanding of the facts, implications, and consequences of maintaining an individual's information within Pinellas HMIS. This includes the sharing of this information with other Member Agencies, to include but not limited to the Pinellas CoC and Homeless Leadership Alliance of Pinellas (HLA). To give informed consent, the individual concerned must have adequate reasoning.

The individual has the right to not share certain data elements with other Member Agencies and this preference would be indicated on the Pinellas HMIS Informed Consent and Release of Information. The signed form would then be submitted by the Member Agency obtaining the release to Pinellas HMIS through the Pinellas HMIS Help Desk ticketing. Once Pinellas HMIS receives the form with sharing restrictions indicated, the visibility of the client's data is updated according to the individual's permissions.

Should there be person-to-person contact that is non-Street Outreach related, i.e., intake, case management, service setting, the original signed Pinellas HMIS Informed Consent and Release of Information should be kept by the Pinellas HMIS Member Agency and protected from theft or loss. The form must be completed by each member of the household receiving services who is over the age of 18. The head of household (HOH) may sign for any children or members of the household under the age of 18 on the same form. Once the signed Pinellas HMIS Informed Consent and Release of Information is obtained, it must be recorded in Pinellas HMIS and is valid until the client revokes or chooses to change their consent.

Client procedures from each Member Agency, including the Pinellas HMIS Informed Consent and Release of Information, must be on file at each agency.

Each Member Agency must publish the most current Pinellas HMIS Privacy Notice, describing policies and practices for the processing of National Privacy Requirements as set forth under the Health Insurance Portability and Accountability Act of 1996, 45 C.F.R., Parts 160 & 164 and corresponding regulations established by the U.S. Department of Health and Human Services is required to operate in accordance with HIPAA regulations and must provide a copy of this Privacy Notice to any individual upon request. If the Member Agency maintains a web page, the current privacy notice must be posted. An amendment to the privacy notice regarding use or disclosure will be effective with respect to information processed before the amendment, unless otherwise stated. All amendments to the Privacy Notice will be consistent with the requirements of these privacy standards. Pinellas HMIS will maintain permanent documentation of all privacy notice amendments.

Member Agencies are obligated to provide reasonable accommodation for persons with disabilities throughout the data collection process. This may include but is not limited to, providing qualified sign language interpreters, readers, or materials in accessible formats such as Braille, audio, or large type, as needed by the individual with a disability. In addition, Member Agencies that are recipients of federal financial assistance shall provide required information in languages other than English that are common in the community, if speakers of these languages are found in significant numbers and come into frequent contact with the program.

The HMIS Privacy Notice will specify the purposes for which the agency collects data and describes uses and disclosures. A Member Agency may use or disclose client data from the Pinellas HMIS only if the use or disclosure is allowed by the HUD's HMIS Data and Technical Standards Final Notice (§ 4.1.3) and is described in the Privacy Notice. HIPAA regulations receive precedence over the HMIS Data and Technical Standards Final Notice.

A Member Agency must allow an individual to inspect and to have a copy of any data about the individual. A Member Agency must offer to explain any information that the individual may not understand. While a Member Agency must consider any request by an individual for correction of inaccurate or incomplete data pertaining to the individual, the Member Agency is not required to remove any information but may alternatively choose to mark information as inaccurate or incomplete and may supplement it with additional information.

A Member Agency, in accordance with HUD's HMIS Data and Technical Standards Final Notice, may reserve the ability to rely on the following reasons for denying an individual inspection or copying of the individual's protected personal information (PPI): (1) Information compiled in reasonable anticipation of litigation or comparable proceedings; (2) information about another individual (other than a health care or homeless provider); (3) 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 (4) Information, the disclosure of which would be reasonably likely to endanger the life or physical safety of any individual. Also, a Member Agency may reject repeated or harassing requests for access or correction and if denied 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 as part of the PPI about the individual.

Client interactions are a fundamental component of the informed consent process. Pinellas HMIS Policy requires written and/or verbal consent as outlined in the Privacy Notice. During a State of Emergency in Pinellas County, verbal consent can be obtained from clients for all partner agencies with the approval of the Continuum of Care (CoC). Except for first party access to information and any required disclosures for oversight of compliance with Pinellas HMIS Privacy and Security Standards, all users and disclosures are permissive and not mandatory. Uses and disclosures not specified in the HMIS Privacy Notice can be made only with the consent of the individual or when required by law. Data may be shared without the client's consent in instances of serious threats to health or safety if it is believed that 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 (HUD's HMIS Data and Technical Standards Final Notice § 4.1.3).

Oral Explanation of Pinellas HMIS and Verbal Consent
Oral Explanation: All clients will be provided with an oral explanation of the Pinellas HMIS and terms of consent by the Member Agency. The Member Agency is responsible for ensuring that this procedure takes place **prior** to every client interview or entry into Pinellas HMIS.

The oral explanation must contain the following information:

1. What the CoC uses Pinellas HMIS for:
    - Understanding Member Agency's clients' needs;
    - Assisting in planning for appropriate resources to better serve consumers; and
    - Informs public policy to end homelessness.

2. The Pinellas HMIS is a computer-based information system that Member Agencies across the county use to capture information about the persons they serve.
    - Client information is transferred in an encrypted format to the Pinellas HMIS database.
    - Clients have the right to not answer any question, **unless entry into a Member Agency program requires it.**
    - Clients have the right to know who has added to, deleted, or edited their Pinellas HMIS electronic client record.

3. Only Member Agency staff who work directly with clients and/or have administrative responsibilities can look at, enter, or edit client records.

4. Benefits for clients:
    - Allows case manager to tell the client what services are offered on site or by referral through the assessment process
    - Assists the case manager and client in obtaining other resources that will help them find and keep permanent housing

The use of **verbal consent** by the client is currently only allowable by approved HMIS projects and notated on the current Privacy Notice. During a State of Emergency, where the ability to meet face-to-face with clients may pose a threat to health and safety, the CoC will expand the use of the verbal consent to other providers. A verbal consent shall be recorded in HMIS and is **valid for one (1) year**.

Verbal Client Consent to Share Data
Each Client whose record is being shared electronically with another Member Agency must agree via verbal consent to have their data shared. A client must be informed what information is being shared and with whom it is being shared. A client must also be informed of the expiration date of the consent. The program types approved for the use of verbal consent can be found on the most current Privacy Notice.

Written Client Consent to Share Data
Each Client whose record is being shared electronically with another Member Agency must agree to share their information by signing a Pinellas HMIS Informed Consent and Release of Information. If the client opts to restrict any of their information the client should indicate this on the signed form which the Member Agency would then send to Pinellas HMIS to restrict visibility in the system. A client must be informed what information is being shared and with whom it is being shared. A client must also be informed of their ability to change, or revoke, their consent in the future.

Policy 2-6: Confidentiality

All standards described in this manual pertain to any homeless assistance organization that records, uses or processes personally identifying information (PII) for Pinellas HMIS. One exception exists to this policy: any Member Agency covered under HIPAA is not required to comply with the standards in this manual if the Member Agency determines that a substantial portion of its PII about homeless clients or homeless individuals is protected health information (PHI) as defined in the HIPAA rules (Section 4.1.2, 2004 HMIS Data and Technical Standards).

Confidentiality Procedures

Member Agencies must comply with HIPAA rules instead of Pinellas 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. Exempting HIPAA covered entities from the HMIS privacy and security rules avoids all possible conflicts between the two sets of rules.

Informed consent includes both an oral explanation and written client consent for each client. All Pinellas HMIS Member Agencies must obtain consent from all clients for whom they are entering or accessing client data into HMIS. Data is also collected and shared when verbal consent is obtained specifically in the case of the Diversion Teams, Street Outreach, and 211 Homeless Helpline. In the event of a declared emergency, verbal consent can be obtained from clients for all partner agencies with the approval of the Continuum of Care (CoC).

All records dealing with clients must be treated as confidential. All Pinellas HMIS users and Agency Administrators are responsible for maintaining the confidentiality of information relating to client information entered into Pinellas HMIS. Failure to maintain confidentiality may result in termination of Pinellas HMIS licenses for the organization.

Pinellas HMIS Corrective Action
Data Security is the highest priority of Pinellas HMIS, but Data Quality is also an essential function of the CoC required for service coordination and improving program performance. Per the U.S. Department of Health and Human Services (2013), a breach is, generally, an impermissible use or disclosure under the HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414 that compromises the security or privacy of the protected information. An impermissible use or disclosure of protected information is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected information has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the protected information involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the protected information or to whom the disclosure was made;
3. Whether the protected information was acquired or viewed; and
4. The extent to which the risk to the protected information has been mitigated.

Critical Risk includes data breach, repeated Medium Risk (3 within 30 days), failure to complete Releases of Information and report Domestic Violence to the HMIS Lead or Security Officer.

Medium Risk includes inaccurate bed count, duplicative entries for clients, accessing inappropriate client records, continually entering benchmark or HUD Universal Data Elements incorrectly for three or more months, failure to notify HMIS Staff of staff departure, etc.

Low Risk includes unresponsiveness to HMIS staff requests, failure to accurately submit the monthly data quality certifications in a timely manner for three or more months consecutively.

Upon notification of a procedural violation, HMIS staff will investigate within one business day and if confirmed, will report to the Security Officer/HMIS Lead who implements action.

In emergency situations, i.e., security breach, imminent danger to the database or other Critical Risk, the Security Officer immediately contacts and reports to the HLA CEO, who has final authority for the impending action. HMIS Governance is notified within one business day of a critical risk.

In instances involving data quality certification issues, the Data and System Performance committee is notified at the next scheduled committee meeting with regard to the risk assessment completed by the HMIS Lead. This would include the action steps required for the Corrective Action Plan. Communication leading up to a training or corrective action plan will be handled on a case-by-case basis.

In all other instances, HMIS Governance is notified at their next scheduled meeting and the HMIS Security Officer implements a course of action outlined in the following steps:

Action Step 1: Consultation with the Provider Agency
Action Step 2: Notification of HLA CEO
Action Step 3: Written warning
Action Step 4: Sanctions
Action Step 5: Probation
Action Step 6: Suspension
Action Step 7: Termination

Action Step 1: Consultation with the Provider Agency.

a) Security Officer/HMIS Lead contacts the Provider Agency Administrator and discusses the inappropriate practice.
b) Security Officer/HMIS Lead and Provider Agency Administrator itemize specific requirements for corrective action.
c) Security Officer/HMIS Lead and Provider Agency Administrator identify a time frame for implementation and completion of the corrective measure(s).
d) Provider Agency Administrator coordinates further training if deemed necessary.
e) Security Officer/HMIS Lead documents conversation and reports this information to the HMIS Data & Support Specialist for tracking purposes.
f) Alerts the HMIS Team to begin monitoring the inappropriate practice, which remains in place until resolution.
g) HMIS Data & Support Specialist informs the Security Officer/HMIS Lead when the corrective action is resolved.
h) Security Officer/HMIS Lead notifies Provider that the corrective action is resolved.

Action Step 2: Notification of HLA CEO

a) Security Officer contacts the HLA CEO and reports on the ongoing corrective action.

Action Step 3: Written Warning

a) If any corrective measures do not happen, or if inappropriate practices continue over multiple months, then the Security Officer/HMIS Lead implements a warning procedure.
b) The Security Officer or an appropriate HMIS staff member (under the Security Officer's instruction or, in the case of a Data Quality issue, the HMIS Lead) sends a notice to the Provider Agency Administrator which includes:
    - An explanation of violations and itemizes specific requirements for improvement as defined through a Corrective Action Plan.
    - A time frame for implementation and completion of the corrective measure(s).
    - A training or technical assistance plan, if deemed necessary.
    - Further HMIS actions if the inappropriate practice(s) continue.
c) The technical support staff archives a copy of the warning in the Provider Agency's file.

Action Step 4: Sanctions

a) If the Provider Agency fails to provide satisfactory responses to the warning within the allotted time period, as defined in the Corrective Action Plan, then the Security Officer reviews all previous correspondences and/or Provider Agency corrective action responses and determine sanctions based on the evidence.
a) The Security Officer notifies the Provider Agency of impending sanctions, the effective date and a copy of the original notice.
b) The HMIS Data & Support Specialist archives a copy of the sanctions notification in the Provider Agency's file.

Any Agency User found to be in violation of security protocols may be sanctioned accordingly.

Sanctions may include but are not limited to: submission of a plan of correction, a formal letter of reprimand, suspension of HMIS privileges, revocation of HMIS privileges, termination of the HMIS Participation Agreement, and civil or criminal prosecution.

A revoked Agency User may be subject to discipline by the Agency pursuant to the Agency's personnel policies.

Action Step 5: Probation

a) If the Provider Agency fails to provide satisfactory responses to the sanctions within the allotted time period, then the Security Officer reviews all previous correspondence and Provider Agency corrective action responses and determine warranted probation.
b) The Security Officer notifies the Provider Agency of impending probation and the effective date.
c) Security Officer assigns designated HMIS staff to work with and monitor resolution of identified areas of violation.

The **notification**:

a) Explains the violation(s) and itemizes specific requirements for improvement.
b) Identifies assigned HMIS staff, who will work collectively with the Agency Administrator and Executive Director, to determine the reason(s) for ineffective corrective measures and create a timeline for effective resolution.
c) Includes a copy of the Security Officer's review of the Provider Agency's issues.
d) Explains the change in provider status to Probationary Provider Agency.

e) The probationary period remains effective until all corrective measures meet the Security Officer's approval and will not persist past one hundred and eighty (180) days from the notification date.
f) The HMIS Data & Support Specialist archives a copy of the probation notification in the Provider Agency's file.

Action Step 6: Suspension

a) If the Probationary Provider Agency's inappropriate practice(s) continues or reoccurs, and there is no resolution with the Security Officer and HMIS staff then the Security Officer begins the suspension process.
b) The HMIS Lead:
    1) Notifies the Provider Agency of impending suspension and the effective date
    2) Assigns appropriate HMIS staff to facilitate data identification and data transfer to another database.
    3) Immediately inactivates all Provider Agency End-user database access
    4) Only reactivates End-user access after receiving written permission via email or fax from HMIS Governance.

    The **notification**:

    1) Identifies assigned HMIS staff, who will work collectively with the Provider Agency Administrator and Executive Director, to identify and transfer database elements needed for the Provider Agency to continue conducting business.
    2) Includes an updated copy of the Security Officer's review and decision to suspend Provider Agency's HMIS access.
    3) Explains the change in provider status to Suspended Provider Agency and the suspension of all End-user database access.
    4) Explains the requirement of a mandatory meeting to address the resolution of inappropriate practices. The HMIS Security Officer coordinates the meeting time and place with all participants, which include the Agency Administrator and/or the Executive Director.

c) The HMIS Data & Support Coordinator archives a copy of the suspension notification in the Provider Agency's file.

Action Step 7: Termination

a) If the Probationary Provider Agency refuses to attend the mandatory meeting or comply with HMIS Policy and Procedures, then HMIS Governance issues an order to the Security Officer to permanently terminate the Provider Agency access to the HMIS database.
b) Data Transfer
    - The Terminated Provider Agency
        1. Must submit a request for their data within 60 days of termination.
        2. Assumes responsibility for cost of data transfer to another database.
        3. Pays the HLA accountant prior to data delivery.

Policy 2-7: Information Security Protocols

To protect the confidentiality of the data and to ensure its integrity at the site whether during data entry, storage and review or any other processing function, a Member Agency must develop rules, protocols or procedures.

Information Security Protocol Procedures

A Member Agency, at a minimum, must address all rules, protocols, or procedures as follows:

- Assignment of user accounts
- Unattended workstations
- Physical access to workstations
  - The implementation of hardware and/or software firewall to secure local systems/networks from malicious intrusion
- Use of Antivirus Software, including the automated scanning of files as they are accessed by users on the system where the Pinellas HMIS application is used as well as assuring that all client systems regularly update virus definitions from the software vendor
- Computer Operating Systems are regularly updated for security and critical updates provided by the software vender
- Use of Anti-Spy ware, including the automated scanning of files as they are accessed by users on the system where the Pinellas HMIS application is used as well as assuring that all client systems regularly update virus and spy ware definitions from the software vendor
- Password complexity, expiration, and confidentiality
- Policy on users not sharing accounts
- Client record disclosure
- Report generation, disclosure, and storage

Policy 2-8: Connectivity

It is the responsibility of the Member Agency to obtain, at minimum, a Broadband Internet connection. T-Lines, Optical Carriers, DSL, Satellite, Integrated Services Digital Networks, and cable internet connections as also acceptable. Free or public wireless hotspots should not be used while accessing Pinellas HMIS or any confidential information obtained from Pinellas HMIS.

Connectivity Procedures

Because vast amounts of data are transmitted, to avoid staff frustration and to be efficient, obtaining and maintaining a broadband (high-speed) Internet connection (greater than 56K/v90) is required. Suggestions include DSL (Digital Subscriber Line), Cable Access, Fiber Optic, or Satellite Downlink.

Policy 2-9: Maintenance of Onsite (Agency) Computer Equipment

The CEO/Executive Director or designee of each Member Agency is responsible for the maintenance and disposal of on-site computer equipment and data used for participation in the Pinellas HMIS.

Computer Equipment Maintenance Procedures

1. **Computer Equipment**: The Member Agency is responsible for maintenance of on-site computer equipment. This includes purchase of and upgrades to all existing and new computer equipment for utilization in the Pinellas HMIS Project.

2. **Backup**: While the Pinellas HMIS system is an internet based, system, and thus all application-level data backups are the vendor's responsibility, each local system is also subject to failure. The Member Agency is responsible for supporting a backup procedure for each computer connecting to the Pinellas HMIS. A backup procedure may include archival of old existing data, and other general backups of user documents and files.

3. **Internet Connection**: The Member Agency is responsible for troubleshooting problems with Internet Connections.

4. **Data Disposal**: The Member Agency agrees to dispose of documents that contain identifiable client level data in a manner that will protect client confidentiality. Methods may include:

    - Shredding paper records;
    - Deleting any information from media and destroying the media before disposal; and/or
    - Triple formatting hard drive(s) of any machine containing client-identifying information before transfer of property and/or destruction of hard drive(s) from any machine containing client-identifying information before disposal.

5. **Data Retention**: Protected Personal Information (PPI) that is not in current use seven years after the PPI was created or last changed must be deleted unless a statutory, regulatory,

contractual, or other requirement mandates longer retention. Care must be taken to assure the guidelines associated with data disposal are properly followed.

Policy 2-10: Universal and Program-Specific Data Elements

The Pinellas HMIS requires each HMIS Member Agency to enter client level data based on a set of predefined data standards. All Member Agency providers are encouraged to record all Universal and Program-Specific Data Elements (UDE & PSDE) for all clients entered into Pinellas HMIS even if not required for funding.

Universal Data Element (UDE) Procedures

Pinellas HMIS data standards are based on the most current revision of the HUD Homeless Management Information System (HMIS) Data Standards. Each Member Agency is responsible for ensuring that a minimum set of data elements, referred to as the HUD Universal Data Elements (UDEs) as defined by the most current HUD HMIS Data Standards Manual, will be collected and/or verified from all clients at their initial program enrollment or as soon as possible thereafter. Member Agencies are required to enter data into the HMIS as specified in Section 9. HMIS Data Quality Policies and Procedures. The UDEs are all included collectively on the Client Profile, Assessment, and HUD Entry and Exit assessments, which are on the Community Services Entry and Exit screens, respectively. Member Agencies must report client-level UDEs using the required response categories detailed in the "Required Response Categories for Universal Data Elements" section of the most current HUD HMIS Data Standards Manual. The most current version of this document can be found on the **HUD Exchange**.

Every program entering data into Pinellas HMIS is graded based on the following elements: quality, completeness, consistency, accuracy, and timeliness. Data is to be entered into Pinellas HMIS within 72 hours of client receiving services, unless an exemption has been approved by the Pinellas HMIS Manager and later ratified by the Pinellas HMIS Governance Committee, additionally, projects are to strive for 95% or higher completeness rating.

Program-Specific Data Element (PSDE) Procedures

Optional PSDE are a valuable area of the client record and part of case management. The collection of these data elements are often required by Federal Agencies providing funding to a project, as detailed in the relevant funding-specific HMIS Project Manual or as outlined in the most recent version of the HUD Data Standards, found on the **HUD Exchange.** In instances where these are not required, these elements are encouraged to be completed for each client especially if the client is in a housing or financial assistance program. The more complete the client record, the better the information available is to help the client more effectively.

Policy 2-11: Pinellas HMIS Grievance

The Pinellas HMIS Governance Committee holds the final authority for all decisions related to the governance of the Pinellas HMIS System. Decisions made or actions authorized by HLA regarding the Pinellas HMIS which do not satisfy an interested party, including those at the Continuum, agency or client levels, may be brought before the Pinellas CoC Grievance Committee for a decision in accordance with the Pinellas HMIS Grievance Procedure. The Pinellas CoC Grievance Committee members will be assigned by the Pinellas HMIS Governance Committee and members will not have a conflict of interest for the grievance they are to adjudicate.

Client Grievance Procedures

Clients of Member Agencies use the Member Agency's existing grievance procedures regarding unsatisfactory services or use and disclosure of Personal Protected Information (PPI) in the Pinellas HMIS, as these issues are most likely within a Member Agency. It is only when the issue involves the actions of the CoC's Pinellas HMIS operation that the Pinellas HMIS Grievance Procedure is to be used. Additionally, the Pinellas HMIS Grievance Procedure is not intended for use as an "appeal" for a local agency decision.

If a client wants to file a complaint:

1. The Client complaint is to be brought to the attention of the Member Agency's CEO/Executive Director or designee, who shall assist the client in the Grievance Procedure.
2. The complaint is to be stated in writing.
3. The complaint shall be returned to the Agency Administrator, who has the ability and authority to take corrective action.
4. The Client and the Member Agency's Agency Administrator meet with the appropriate Pinellas HMIS party to resolve the complaint.
5. The actions and resolutions shall be in writing.

If the matter cannot be resolved to the satisfaction of all parties, the Pinellas HMIS Governance Committee will convene the Pinellas CoC Grievance Committee, giving them information concerning all actions taken to date:

1. The complaint is forwarded to the Pinellas HMIS Director by the Member Agency's CEO/Executive Director or designee.
2. The Chief Administrative Officer will staff the complaint with the Pinellas HMIS System Administrator and the HLA CEO or designee and prepare a written summary to be forwarded to the Pinellas CoC Grievance Committee.
3. The Pinellas CoC Grievance Committee will meet, a minimum of 14 days, after being notified by the HLA regarding the formal complaint to hear the summary.
4. The Pinellas CoC Grievance Committee will resolve the complaint within five (5) working days after this meeting.
5. Should the client want to appeal the Pinellas CoC Grievance Committee's decision, the Pinellas CoC Grievance Committee will hear the appeal at its next scheduled meeting and resolve the complaint in the manner in which it makes its decisions. This decision is final.
6. All actions and resolutions will be in writing. Both the client and Pinellas HMIS Member Agency involved will have a copy describing the resolution of the complaint.

Grievance by Member Agencies or a Continuum of Care: Member Agencies are to first ascertain if the issue is at the Continuum of Care level and if so to resolve it at that level.

If a Member Agency, Continuum of Care, or any combination of such organizations has a complaint about a decision or an action of the Pinellas HMIS staff concerning the Pinellas HMIS or any issue about which the Pinellas HMIS has responsibility, they should first bring the matter to the attention of the Chief Administrative Officer who has the ability and authority to take corrective action as a verbal, informal Grievance Procedure.

Informal Grievance Procedure

The informal grievance procedure involves bringing the issue verbally to the Pinellas HMIS party who has the ability and authority to take corrective action. It is intended that a meeting between the parties shall resolve the issues.

Formal Grievance Procedure

If the matter is not resolved through the Informal Grievance Procedure to the satisfaction of the Member Agency or Continuum of Care, the Formal Grievance Procedure should be initiated.

1. The complaint should be in writing and submitted to the Pinellas HMIS Governance Committee who will convene the Grievance Committee.
2. The Grievance Committee will meet, at a minimum, of 14 working days to allow for quorum, after being convened and notified of the complaint and will consider information from all parties involved.
3. The Grievance Committee will hear the complaint from all parties.
4. The Grievance Committee will resolve the complaint within five (5) working days.
5. The actions and resolution of the grievance shall be in writing.
6. If the grieving party is not satisfied, the decision may be appealed to the Pinellas HMIS Governance Committee, who will hear and resolve the complaint at its next regularly scheduled meeting. This decision is final.

Policy 3-1: Access Levels for System Users

User accounts will be created and deleted by Pinellas HMIS staff. There are different levels of access to the Pinellas HMIS. These levels are reflective of the access a user has to client level paper records. Access levels should be need based and any prospective Pinellas HMIS user should never have access or view detailed information on program and service participants with whom they were once friends or a fellow participant.

Access Level for System Users Procedures

A Member Agency must require each potential user of Pinellas HMIS (including employees, volunteers, affiliates, contractors and associates) to sign (upon hire, and when modified) a Pinellas HMIS End User Agreement and to acknowledge receipt of a copy of the most current Pinellas HMIS Privacy Notice and to pledge to comply with the privacy notice as issued.

Policy 3-2: Access to Data

Users will be able to view the data entered by Member Agencies in accordance with their respective Participant Agreement. Security measures exist within the Pinellas HMIS system which restricts agencies from viewing data not covered by the executed Participant Agreement.

Requests from Law Enforcement: The Pinellas HMIS staff will not print, give an electronic copy of, or disclose any personal information without a subpoena. Subpoenas are to be submitted to the Pinellas HMIS Manager and include requests for: Next-of-kin searches; searches for clients by family or friend; searches for clients who may be in danger or whose health may be at risk; and searches for clients in the interest of public safety where law enforcement has probable cause or an active warrant for his/her arrest, related to a violent crime and other felony crimes.

Access to Data Procedures

The Member Agencies must establish protocols for internal access to data. These access protocols must contain the following elements:

1. Physical security policies and procedures
2. User security training
   - User orientation
   - Periodic reminders of internal procedures
   - An industry recognized user authentication system
3. Access authorization policies and procedures
4. Access revocation policies and procedures
5. Incident reporting policies and procedures
6. Sanction policies and procedures
7. Termination procedures
8. Risk Assessment
9. Risk Management

Policy 3-3: Access to Client Paper Records

Each agency must secure any paper or other hard copy containing personal protected information that is either generated by or for the Pinellas HMIS, including, but not limited to reports, data entry forms, and signed consent forms.

Client Paper Records Procedures

All paper or other hard copy generated by or for the Pinellas HMIS that contains PPI must be directly supervised when the hard copy is in a public area. When agency 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. All Pinellas HMIS paper records that contain client information must be destroyed seven (7) years after the client has left the program.

Policy 3-4: Unique User ID and Password

All Member Agency Pinellas HMIS user accounts will be the responsibility of their Agency Administrator; Pinellas HMIS staff will grant a unique user ID and password to all Member Agency users once the Agency Administrator acknowledges that they have a license available, submits the necessary paperwork, and the user attends their new user training.

User Id and password procedures

- Each user will be required to enter a Pinellas HMIS assigned User ID and Password in order to access the system. This information is given to the user once they attend the new user training.
- Upon initial access using the assigned information for access, the new user will be prompted to change the Pinellas HMIS assigned password. This is another security measure built into Pinellas HMIS. This user-created password must be no less than eight and no more than ten characters in length which will not be comprised of words, backward words, names, backward names or any identifiable acronym.
- The password must be alphanumeric.
- Users must use industry standard best practices when selecting their password including the following: Use lower- and upper-case letters; and do not use passwords containing the names of a spouse, child or pet (similar names or backward names, places or things) and do not use birthdates or other easy to guess items.
- Written information specifically pertaining to user access, e.g., username and password, may not be stored or displayed in any publicly accessible location.

Password Reset:

- Initially each user will be given a password for one time use only. The first password will be created by Pinellas HMIS staff and will be issued to the User.
- The Member Agency Administrator will reset a password if necessary.
- Unsuccessful logon: If a User unsuccessfully attempts to log in three times, the User ID will be "locked out" on the next attempt and access permission will be locked. The user will be unable to gain access until their password is reset either through their Agency Administrator or through the Pinellas HMIS HelpDesk ticketing system.

Policy 3-5: User Inactivity

To ensure consistent data entry and accurate data, it is important for End Users to actively use Pinellas HMIS. This assists the CoC in making data-driven decisions.

Subsidized Licenses

End Users who have not logged into the system for 30 days will be considered inactive and the End User and Agency Administrator are notified that the profile has been inactivated. The Member Agency Administrator can submit a Help Desk request to have access reinstated between 31st and 60th day. End User accounts not active for 60 days will need to complete the Talent Annual Refresher Training to be reinstated. After the 91st day of inactivity, the end user account will be removed from HMIS, and the Member Agency risks forfeiture of the license if the end user's profile was subsidized. The license will be temporarily unavailable until HMIS Governance makes the final decision of forfeiture.

Unsubsidized Licenses

End Users who have not logged into the system for 30 days will be considered inactive and the End User and Agency Administrator are notified that the profile has been inactivated. The Member Agency Administrator can submit a Help Desk request to have access reinstated between 31st and 60th day. End User accounts not active for 60 days will need to complete the Talent Annual Refresher Training to be reinstated. After the 91st day of inactivity, the end user account will be removed from HMIS. The inactivated license will be reinstated to the Member Agency for future usage.

Policy 3-6: Right to Deny User and Member Agency Access

The Member Agency or user access may be suspended or revoked for suspected or actual violation of the security protocols. Serious or repeated violation by users of the system may result in the suspension or revocation of an agency's access.

Right to deny user procedure:

1. Criminal or illegal activity in which a client's rights, privacy, safety, or security has been violated take precedence for resolution over all other data violations.
   a. Policies and Procedures concerning criminal and/or illegal activities are addressed in the Pinellas CoC Lead Agency System Policies and Procedures.
2. The agency and their Pinellas HMIS System Administrator will investigate all suspected violations of any security protocols.
3. Any user found to be in violation of security protocols will be sanctioned by his/her agency. Sanctions may include but are not limited to a formal letter of reprimand, suspension of system privileges, revocation of system privileges, termination of employment and/or criminal prosecution.
4. It is the responsibility of the Member Agency Administrator to report any violations within 24-business hours to the Pinellas HMIS System Administrator.
5. Pinellas HMIS may restrict access prior to completion of formal investigation if deemed necessary by the Pinellas HMIS System Administrator. If access is restricted, the Pinellas HMIS System Administrator or Performance Improvement Manager will notify the Member Agency CEO and the chair of the HMIS Governance committee of the restriction to consult with them about next steps.
6. Any agency that is found to have consistently and/or flagrantly violated security protocols may have their access privileges terminated.
7. If the Pinellas HMIS Member Agency violates any policies deemed of critical risk and fails to achieve resolution within a timeframe prescribed by the HLA, the Pinellas HMIS staff will permanently terminate the Member Agency from Pinellas HMIS. The Pinellas HMIS Member Agency's CEO/Executive Director will receive a written notice, via certified mail, regarding the Termination, reasons and effective date. A copy of the notification of the termination will be sent to all funders associated with the project in question. In the case there are data quality costs and/or transfer costs, the Member Agency may assume responsibility for payment.
8. All sanctions can be appealed to the Pinellas CoC Grievance Committee.
9. Member Agencies seeking to be returned to full active Pinellas HMIS status, after being terminated must complete a reinstatement process that includes full training for all users and Agency Administer; and a 12-month probationary period. Member agencies requesting their PHMS license be re-instated after license has been suspended by the HLA may be responsible for the cost to re-activate the license. This determination will be made by the Pinellas HMIS Governance Committee.

Policy 3-7: Data Access Control

Agency Administrators at Member Agencies and the Pinellas HMIS staff reserve the right to monitor access to Pinellas HMIS software.

Data Access Control Procedures

Agency Administrators at Member Agencies and the Pinellas HMIS staff will regularly review Pinellas HMIS user access privileges and deactivate users when users no longer require access. Pinellas HMIS staff will monitor all user licenses and usage quarterly, and review and set licensing fees for the Pinellas HMIS system annually.

It is the responsibility of the Pinellas HMIS Member Agency's Agency Administrator to notify Pinellas HMIS when licenses are not being used by agency staff, when there is a turnover or termination of agency staff that will impact the name on a license, and for purchasing additional licenses when needed. Pinellas HMIS Member Agencies are to notify Pinellas HMIS within five (5) business days of any licensing changes. Pinellas HMIS staff will run a Pinellas HMIS License Usage Report on a quarterly basis assisting Pinellas HMIS staff with the addressing the following:

- Pinellas HMIS Member Agency Administrators will be contacted when the system identifies a license that has not been used in the past 90-days. Pinellas HMIS Member Agency Administrators will have 48 hours to confirm with Pinellas HMIS if this license is still needed by the agency. If Pinellas HMIS does not receive a response from a Member Agency within the 48-hour timeframe, the license will be inactivated and put into the Pinellas HMIS License Pool.
- All requests for new or additional user licenses must be submitted in writing to the Pinellas HMIS HelpDesk ticketing system. Once notice has been received, Pinellas HMIS staff will advise if the Member Agency has an available license. If a license is not available, Pinellas HMIS staff will contact the vendor and purchase the licenses as well as notify the HLA Finance Director if license billing/invoicing is required. If additional licenses need to be purchased, licenses will be provided once payment is received.
- Agency Administrators at Member Agencies and Pinellas HMIS staff may implement discretionary access controls to limit access to Pinellas HMIS information based on application security designations. Examples of such designations include but are not limited to "Agency Administrator", "Case Manager", and "Volunteer."
- Agency Administrators at Member Agencies and Pinellas HMIS staff may audit unauthorized accesses and attempts to access Pinellas HMIS information. The access records shall be kept at least six months, and Agency Administrators and the Pinellas HMIS Systems Administrator may review the audit records for evidence of violations or system misuse.

Guidelines for data access control for the Member Agency: The federal regulations state that physical access to systems with access to computers that are used to collect and store HMIS data shall be staffed at all times when in public areas. 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 publicly accessible. These steps should **minimally include:**

- Logging off the data entry system, shutting down the computer, and storing the computer and data in a locked room. This could be accomplished using an operating system with individual profiles and system security policies enabled
- Any passwords written down should be securely stored and inaccessible to other persons. Users should not store passwords on a personal computer for easier log on.

Policy 3-8: Using Pinellas HMIS Data for Research

Member Agencies in the Pinellas HMIS should collect personal client information only when appropriate to provide services and/or for other specific purpose of the organization and/or when required by law.

Pinellas HMIS Data for Research Procedures:

Purposes for which agencies collect protected personal information may include the following:

- To provide or coordinate services to clients;
- Locate other programs that may be able to assist clients;
- For functions related to payment or reimbursement from others for services that are provided;
- To operate the agency, including administrative functions such as legal, audits, personnel, oversight, and management functions;
- To comply with government reporting obligations when required by law; and
- For research purposes.

Pinellas HMIS Release of Data for Research Conditions

The Pinellas HMIS Governance Committee will review and respond to requests for the use of Pinellas HMIS data for research:

- No client protected personal information for any reason may be released to unauthorized entities.
- Only de-identified aggregate data will be released.
- Aggregate data will be available in the form of an aggregate report or as a raw data set. Parameters of the aggregate data, that is, where the data comes from and what it includes, will be presented with each report.
- Research results will be reported to the Pinellas HMIS Governance Committee for approval prior to publication by the HLA.
- Research will be shared with the appropriate agencies after publication.
- The HLA will be granted the rights to utilize all findings (results).

Policy 3-9: Pinellas HMIS Roles and Descriptions/System Administrator II

HLA, not limited to HMIS, staff facilitating case conferencing will be assigned as System Administrator Level II roles in order to review data related to clients' history within the Pinellas HMIS. This information will include, but is not limited to client program enrollments, services, and case plan notes.

Roles and general descriptions of the capabilities of each role are listed below.

- Read-Only Access Users: These users can view, but not edit any screens within the Clients module. User may access Reports.
- HMIS Case Manager (I, II or II): Users may access all screens and modules except "Administration." A Case Manager may access all screens within the Clients module, including viewing and editing Client Level information shared within HMIS.

- HMIS Agency Administrator: In addition to the level of access as a Case Manager, Agency Administrators may access all Community Services screens and modules available to their agency and projects (granted by the HMIS Lead Agency). Agency Administrators may access and reset users passwords in HMIS. This function is limited to users within that Administrator's agency.
- Executive Director: Users have the same access rights as an Agency Administrator but rank above the Agency Administrator.
- System Administrator (I or II): There are no system restrictions for this role. They have full HMIS access.

Section 4: Data Quality and Monitoring

Policy 4.1: Pinellas HMIS Data Quality Policy

Pinellas HMIS Member Agency providers will work diligently to adhere to data quality standards set forth by the CoC to ensure that reports both at the provider level and the system level are complete, consistent, accurate, and timely.

Pinellas HMIS Data Quality Procedures

The HLA is responsible for implementing data standards in such a way that specifies the data quality standard to be used by all Member Agencies; provides a mechanism for monitoring adherence to the standard; and provides the necessary tools and training to ensure compliance with the standard. This includes strategies for working with agencies that are not in compliance with the Pinellas HMIS Data Quality standards.

Data Quality Standards

- All names provided will be accurate based on client self-report unless agency is able to verify name with social security card or other government-issued document;
- Blank entries in required data fields will not exceed the error rate for their project type as outlined in the **Pinellas HMIS Data Quality Plan**;
- Data inconsistencies or missing data will not exceed the HUD error rate for their project type as outlined in the **Pinellas HMIS Data Quality Plan**;
- All client data should be entered no later than 72 business hours after intake, assessment, or program or service entry or exit;
- In the event Pinellas HMIS users are not able to enter data in real time, data should be backdated to ensure that the data entered reflects the actual client service provision dates;
- All client data entered into Pinellas HMIS must match the Member Agency's client record/case file;
- Pinellas HMIS users should not assume client data or make changes to client data not reported by the client unless the information has been officially verified. Examples of verification include, but are not limited to, documents such as: Social Security Cards; Government-issued IDs; SSI/SSDI benefit letters; and/or letters of employment or paystub information;
- All Universal Data Elements must be obtained from each adult and unaccompanied youth who applies for services through the CoC. Most Universal Data Elements are also required for children age 17 years and under. More information on data collection for the Universal Data Elements can be found in the **HUD Data Standards Manual**;
- HLA staff, including, but not limited to, the Pinellas HMIS Staff and HLA Performance Improvement Manager, will conduct a monthly data review for all projects utilizing the Entry/Exit workflow;
    - Any data errors or concerns that are identified during this monthly data review will be reported to the Member Agency's Agency Administrator for clarification or correction;
    - Member Agencies must maintain a Completeness grade of 95% or above for client information entered into Pinellas HMIS;
    - If the error rating for a project rises above the acceptable target error percentage (as outlined in the **Pinellas HMIS Data Quality Plan**), the HLA will create a training course of action for the agency's Pinellas HMIS users;
    - If the error rating for a project continues to rise above the acceptable target error percentage (as outlined in the **Pinellas HMIS Data Quality Plan**), the HLA may implement corrective action, which would be monitored by the Data System and Performance Committee;

- Agency Administrators will receive training on how to run and read the reports necessary for completion of the Pinellas HMIS Data Certification process, as outlined in the **Pinellas HMIS Data Quality Plan**;
- Bed inventory should be consistently maintained and managed to reflect true occupancy rates. Changes to the Member Agency's bed inventory must be reported on the monthly HMIS Data Quality Certification;
- Inventories need to be sent to the Pinellas HMIS System Administrator within five (5) business days of any changes;
- Pinellas HMIS Staff will manage a centralized bed inventory;
- Agencies will be required to submit updated bed inventories to the Pinellas HMIS System Administrator quarterly, even if there have been no inventory updates;
- Any data errors identified by Pinellas HMIS staff that have been submitted to the Member Agency's Agency Administrators needs to be corrected within the time frame outlined by Pinellas HMIS staff;
- Pinellas HMIS end users must conduct a search for existing clients in the system before adding a new client into the system;
- All client data should adhere to the Pinellas HMIS style guidelines (https://pinellashmis.zendesk.com/hc/en-us/articles/115002836173-Pinellas-HMIS-Style-Guide);
- If a client stays in an Emergency Shelter for less than six (6) hours the data should not be entered into Pinellas HMIS. Same day enrollments and exits in Emergency Shelter with **no bed night stay should not be entered** in Pinellas HMIS;
- Member Agencies should inform Pinellas HMIS staff through the Pinellas HMIS HelpDesk if a client did not stay for 6 hours or longer or did not stay overnight so the data can be removed. Pinellas HMIS staff will periodically check for clients who meet the above criteria and remove the enrollment as the policy dictates.
- When duplicate information, such as duplicate client records, is found, the Member Agency will notify Pinellas HMIS immediately through the Pinellas HMIS HelpDesk.

Policy 4.2 Data Quality Monitoring

The Pinellas HMIS staff will perform weekly, monthly, quarterly, and annual data integrity checks on the Pinellas HMIS data.

Data Quality Monitoring Procedures

Programs should run their Pinellas HMIS Data Quality Certification reports on a weekly basis and the Annual Performance Report (APR) or equivalent annual report (example: Emergency Solutions Grant Consolidated Annual Performance and Evaluation Report (ESG-CAPER) monthly. Pinellas HMIS is responsible for reporting system errors and difficulties with HMIS working processes to the vendor/software provider. The vendor/software provider must make all functionality changes to the system and these changes are not able to be completed by Pinellas HMIS Staff.

Pinellas HMIS Staff will run HUD Universal Data Elements, Data Incongruities Reports, and other data quality reports as determined by the CoC to determine any patterns or data errors. On a monthly basis, Pinellas HMIS staff and programmatic HLA staff will review the Data Quality Certifications submitted by each Member Agency during Internal Data Review. If error ratings for a project rise above the acceptable target error percentage, Pinellas HMIS will create a training course of action for the Pinellas HMIS users and Member Agency Administrator. If error ratings for project continues to rise above the acceptable target error percentage, the Pinellas HMIS may implement corrective action, which would be monitored by the Data and System Performance Committee and reported to the Pinellas HMIS Governance Committee during their next regularly scheduled meeting. Pinellas HMIS is available to provide technical assistance upon request through the Pinellas HMIS HelpDesk ticketing system.

Pinellas HMIS staff will conduct weekly reviews for duplicate data entries into the system and merge client records. Pinellas HMIS users are encouraged to notify Pinellas HMIS staff when duplicative data is found by way of the HelpDesk ticketing system or through their designated Agency Administrator.

Pinellas HMIS will notify a Member Agency CEO/Executive Director if their Agency Administrators are not responsive to required corrective actions. If data quality issues or unresolved corrective actions continue, Pinellas HMIS will notify the HLA CEO, CoC Chair, and the Pinellas HMIS Member Agency CEO/Executive Director for resolution. If a resolution cannot be reached the non-compliance issue will be addressed at HMIS Governance.

Accountability for Data Quality

If during the HMIS monthly Internal Data Review a pattern(s) of error(s) is identified it will be reported to the (Member) Agency Administrator through email advising them that they will be required to correct the data and that a mandatory Pinellas HMIS training specific to the error/trend is conducted for their identified end user(s). These user(s) will be monitored monthly for compliance until the pattern has been resolved, technical assistance will be provided as needed.

A Member Agency may be considered to be out of compliance with their Pinellas HMIS Participant Agreement if they do not demonstrate a good faith effort to make necessary data corrections as soon as possible, but no later than (5) five days of notification (unless arrangements are made for an extension). Noncompliance to address data entry errors may result in a suspension of the Member Agency's Pinellas HMIS user licenses.

Section 5: Technical Support and System Availability

Policy 5-1: Technical Support

The Pinellas HMIS staff is responsible for providing technical support to Pinellas HMIS Member Agency Administrators and users. Technical support services are available to help users solve specific problems with a product, but do not include customization, reporting, or other support services.

Technical Support Procedures
Pinellas HMIS staff, in conjunction with Member Agency Administrators and/or contracted third parties, will coordinate technical support services on a planned schedule to:

- Assist Member Agencies on the use of Entry/Exit forms and other paperwork
- Conduct follow-up training if needed
- Coordinate follow-up data entry training if needed
- Review report generation
- Coordinate ongoing technical assistance as needed
- Assist agencies with network and end user computer security
- Create custom reports, in accordance with Pinellas HMIS Governance Committee guidelines

Member Agency Service Request: To effectively respond to service requests, the following methods of communicating a service request from a Member Agency to Pinellas HMIS staff have been developed:

1. Member Agency user informs their Agency Administrator of the problem.
2. Member Agency's Administrator attempts to resolve issue and if unable to resolve, contacts Pinellas HMIS staff to request service through the HelpDesk ticketing system.
3. Pinellas HMIS staff determines resources needed for the service request and if necessary, contacts vendor for support.
4. Pinellas HMIS staff will contact the Member Agency's Agency Administrator to work out a mutually convenient service schedule and resolution to issue or concern.

Chain of communication: *(Problems should be resolved in the order given to assure minimum time to resolution. Issues resolved at the higher level will be communicated back through the chain in reverse order.)*

1. End User
2. Member Agency Administrator
3. Pinellas HMIS HelpDesk
4. Pinellas HMIS System Administrator
5. HLA Chief Administrative Officer

Policy 5-2: Pinellas HMIS Staff Availability

Consistent with the user's reasonable service request requirements, HLA Pinellas HMIS staff is available for Technical Assistance, questions, and troubleshooting between the hours of 8:30 AM and 5:00 PM Monday through Friday.

Emergency Situations
Outside of normal business hours (8:30 AM to 5:00 PM Monday through Friday), users should contact the Pinellas HMIS HelpDesk and send a detailed message. Pinellas HMIS staff will respond within 24 business hours.

Section 6: Training Information

Policy 6-1: Pinellas HMIS Training Descriptions

- Pinellas HMIS Agency Administrator Training
- Pinellas HMIS New User Training – Clients
- Pinellas HMIS New User Training – Shelters
- Pinellas HMIS Follow-Up Training
- Pinellas HMIS Basic Report Training
- Pinellas HMIS Intermediate Report Training
- Pinellas HMIS Annual Refresher Training Courses

Pinellas HMIS Agency Administrator Training

***Prerequisite**:* An executed HMIS Agency Administrator Designation form must be on file with Pinellas HMIS identifying the Agency Administrator by the Member Agency prior to training. Prior to gaining Pinellas HMIS access as an Agency Administrator, the end user will be required to submit new user paperwork as well as a Security Awareness Certificate and a HIPAA Basics Certificate. The Agency Administrator must also receive the Pinellas HMIS New User trainings that apply to their agency's HMIS projects and be trained on Basic Reporting in order to complete the Pinellas HMIS Data Quality Certification process.

Every Agency Administrator must attend Agency Administrator Training. This training is specially designed to teach the Agency Administrator about how to communicate with the Pinellas HMIS staff and manage and monitor their HMIS data. This course covers license monitoring, new license requests, new user paperwork content, and the submission process for new user paperwork. Additionally, the class outlines the expectations required of Agency Administrators and how to request technical assistance from the Pinellas HMIS Staff. Annual Refresher Trainings and a Follow-Up Training are mandatory following this training.

Pinellas HMIS New User Training – Clients

***Prerequisite**:* The Member Agency's Agency Administrator will be required to submit new user paperwork as well as a Security Awareness Certificate and a HIPAA Basics certificate for each user prior to training.

This class focuses on the basic data entry requirements for entering all clients into the Pinellas HMIS Clients module. Training includes a meeting on the current HMIS forms including Informed Consent and Release of Information, and HMIS Privacy Notice. During this training, end users will learn how to create and/or find clients in the system, follow the Entry/Exit workflow, and capture services. Training content can be modified to suit an agency's needs upon request. Annual Refresher Trainings and a Follow-Up Training are mandatory following this training.

Pinellas HMIS New User Training – Shelters

***Prerequisite**:* The Member Agency's Agency Administrator will be required to submit new user paperwork as well as a Security Awareness Certificate and HIPAA Basics certificate for each user prior to training.

This class focuses on the basic data entry requirements for entering all clients into the Pinellas HMIS Shelters module. Training includes a meeting on the current HMIS forms including the Client Informed Consent and Release of Information, and HMIS Privacy Notice. During this training, end users will learn how to create and/or find clients in the system, check in and check

out a client and modify an existing shelter stay. Training content can be modified to suit an agency's needs upon request. Annual Refresher Training Courses and a Follow-Up Training are mandatory following this training.

Pinellas HMIS Follow-Up Training

***Prerequisite**:* HMIS New User Training (Clients or Shelters)

This class focuses on a random sample of an end user's data entry and includes meeting on areas of improvement. Subsequent follow-up trainings may be required.

Pinellas HMIS Basic Report Training

***Prerequisite**:* Must be an active Pinellas HMIS end user before receiving this training. This training is strongly encouraged for all Pinellas HMIS Agency Administrators.

This training is customized to meet the needs of the Agency or end user receiving the training. At a minimum, this training is an overview of the basic reporting tools available, how to access them, and how to run and save reports. This includes the data quality reports necessary to complete the Pinellas HMIS data certification process (see the **Pinellas HMIS Data Quality Plan** for more information) as well as provider reports including the Client Served Report, CoC-APR, and ESG CAPER. Other reports may be included at the request of the Agency or End User who requests the training.

Pinellas HMIS Intermediate Report Training

***Prerequisite**:* Must be an active Pinellas HMIS end user, have completed a basic report training, and have a custom report license.

This is a supplemental training beyond the Pinellas HMIS Basic Report Training. The training includes the basic reporting principles and how to navigate the reporting tools. It will demonstrate the basics on how to create counts, charts, tables, and graphs within the available reporting tool. On-going assistance and support through the Pinellas HMIS HelpDesk will be available in order for a trained user to request a custom report if needed.

Pinellas HMIS Annual Refresher Trainings

***Prerequisite**:* HMIS New User Training (Clients or Shelters)

HMIS users are required to complete the annual HMIS training series consisting of: DCF HIPAA Basics, and Security Awareness Courses; Pinellas HMIS Privacy & Security Course, as well as the HMIS Data Entry course. Failure to complete the above courses will result in an inactive license status until the trainings are completed. These trainings will be assigned to each end-user 30 days prior to the completion deadline. Enrolling end-users in virtual training will help agencies and end-users by keeping refresher trainings' schedules consistent and will allow agencies to internally coordinate staff calendars.

List of Revision Date, Additions, and Deletions to Pinellas HMIS P & Ps

Original Issue	March 2005
Revision 8	October 2012
Revision 9	August 17, 2017
Revision 10	June 7, 2018
Revision 11	June 25, 2018
Revision 12	March 18, 2019
Revision 13	March 25, 2020
Revision 14	February 10, 2021
Revision 15	February 4, 2022
Revision 16	October 1, 2022 (Licensing fees increased by vendor)
Revision 17	February 7, 2023
Revision 18	February 7, 2024

Section 7: Attachments

FACT Sheet: Pinellas Homeless Management Information System (Pinellas HMIS)

Information that you provide will be entered into a computer software program called Pinellas Homeless Management Information System (Pinellas HMIS). This is done for several reasons:

- To find out what is needed to end homelessness in Pinellas County;
- To provide better service(s);
- To receive federal funds.

IMPORTANT POINTS ABOUT HOW YOUR INFORMATION WILL BE USED

- Pinellas HMIS keeps a record of your contact with our agency.
- No information is shared **without your written permission.** A signed Informed Consent and Release of Information form will allow us to share client profile information with other Pinellas HMIS Member Agencies. This means that you will not have to provide the same information at more than one intake.

KNOW YOUR RIGHTS

You have the following rights:

- To review your electronic records within 48 hours.
- To have your record changed so that information is up-to-date and correct.
- To refuse consent and still receive services.
- To file a complaint about how the system was used.

To file a complaint, write to:

Pinellas HMIS Governance Committee
c/o Homeless Leadership Alliance of Pinellas, Inc.
Attn: Chief Administrative Officer
740 4th Street N, Suite 206
St. Petersburg, FL 33701

Security Officer

The Homeless Leadership Alliance of Pinellas, Inc. (HLA) Chief Program Officer designates a member of the Quality and Improvement Team as the Pinellas HMIS (Pinellas HMIS) Security Officer whose duties include:

- Review of the Security Plan annually and at the time of any change to the security management process, the data software, the methods of data exchange, and any Pinellas HMIS data or technical requirements issued by HUD. If changes are required to the Pinellas HMIS Security Plan, the Security Officer will work with the Pinellas HMIS and the Pinellas HMIS Governance Committee for review, modification, and approval.
- Confirmation that the HLA adheres to the Security Plan.
- Response to any security questions, requests, or security breaches to the Pinellas HMIS and communication of security-related Pinellas HMIS information to Member Agencies.

Each Member Agency (MA)'s Agency Administrator must serve as the MA's Pinellas HMIS Security Officer, whose duties include:

- Confirmation that the MA adheres to the Security Plan.
- Communication of any security questions, requests, or security breaches to the HLA Pinellas HMIS Security Officer, and security-related Pinellas HMIS information relayed from the Pinellas HMIS System Administrator to the Member Agency's end users.
- Participate in security awareness training annually.

Annual Security Certification

The HLA and each MA must complete an annual security review to ensure the implementation of the security requirements for the Pinellas HMIS which includes a completion of a security checklist, ensuring that each of the security standards is implemented in accordance with the Pinellas HMIS security plan. Each MA Agency Administrator will complete the Security Self-Certification each January using the attached form and submit the completed form to the HLA Security Officer no later than March 15 of each year.

Security Awareness Training and Follow-up

All users must receive security training prior to being given access to the Pinellas HMIS. The HLA has created an on-line security and privacy training module that is to be completed prior to being issued a password. The request for a new password requires a certification that the new user has completed the on-line training. In addition, the HLA shall provide security training no less than once per year.

Security Incidents

All Pinellas HMIS users are obligated to report to their agency MA Agency Administrator suspected instances of noncompliance with policies and procedures that may leave Pinellas HMIS data vulnerable to intrusion. Each MA is responsible for reporting any security incidents involving the real or potential intrusion of the Pinellas HMIS to the HLA. The HLA is responsible for reporting any security incidents involving the real or potential intrusion of the Pinellas HMIS to the HLA's Chief Executive Office and the CoC's HMIS Governance Committee.

Reporting Threshold

Pinellas HMIS end users must report any incident in which unauthorized use or disclosure of personable identifiable information (PII) has occurred and any incident in which PII may have been used in a manner inconsistent with the MA Privacy or Security Policies. It is the obligation of the MA to report all security breaches that have the possibility to impact the Pinellas HMIS to the Pinellas HMIS Director.

Reporting Process
Pinellas HMIS end users will report security violations to their MA Pinellas HMIS Security Officer. The MA Pinellas HMIS Security Officer will report violations to the HLA Pinellas HMIS Security Officer. Any security breaches identified by WellSky (Community Services) will be communicated to the HLA Pinellas HMIS Security Office and HLA Manager. The HLA Manager will review violations and recommend corrective and disciplinary actions to the Pinellas HMIS Governance Committee, as appropriate. Each Member Agency will maintain and follow procedures related to internal reporting of security incidents.

Audit Controls
WellSky maintains an accessible audit trail within Community Services/ServicePoint that allows the Pinellas HMIS System Administrator to monitor user activity and examine data access for specified end users. The Pinellas HMIS Data Manager and/or System Administrator will monitor audit reports for any apparent security breaches or behavior inconsistent with the Privacy Policy outlined in these policies and procedures.

System Security
Each MA is required to apply system security provisions to all the systems where personal identifiable information is stored, including, but not limited to, a MA's networks, desktops, laptops, smart phones, iPad and tablets, netbooks, mainframes, and servers.

User Authentication
A MA must secure Pinellas HMIS systems with, at a minimum, a user authentication system consisting of a username and a password. Passwords must be at least eight characters long and meet reasonable industry standard requirements.

Using default passwords on initial entry into the HMIS application is allowed so long as the application requires that the default password be changed on first use. Written information specifically pertaining to user access, e.g., username and password, may not be stored or displayed in any publicly accessible location. Individual users cannot log on to more than one workstation at a time or be able to log on to the network at more than one location at a time.

Virus Protection
It is necessary that MA's protect Pinellas HMIS systems from viruses by using commercially available virus protection software. Virus protection must include automated scanning of files as they are accessed by users on the system where the Pinellas HMIS application is housed. A MA's are to regularly update virus definitions from the software vendor.

Firewalls
A MA is also obligated to protect the Pinellas HMIS system from malicious intrusion with a secure firewall. Each individual workstation does not need its own firewall, if there is a firewall between that workstation and any systems, including the Internet and other computer networks, located outside of the organization. For example, a workstation that accesses the Internet through a modem would need its own firewall. A workstation that accesses the Internet through a central server would not need a firewall if the server has a firewall.

Physical Access to Systems with Access to Pinellas HMIS Data
A MA must staff computers stationed in public areas that are used to collect and store Pinellas HMIS data at all times. When workstations are not in use and staff is not present, steps should be taken to ensure that computers and data are secure and not usable by unauthorized individuals. After a short amount of time, workstations should automatically turn on a password-protected screen saver when the workstation is temporarily not in use. If staff from a Contributing HMIS Organization (CHO) will be gone for an extended period, staff should log off the data entry system and shut down the computer.

Hard Copy Security
A MA's staff is to secure any paper or other hard copy containing personal identifiable information (PII) that is either generated by or for Pinellas HMIS, including, but not limited to reports, data entry forms, and signed consent forms. Any paper or other hard copy generated by or for Pinellas HMIS that contains PII located in a public area must have an MA's staff present. When an MA's staff is not present, the information must be secured in areas that are not publicly accessible.

Hard copies of data stored or intended to be stored in Pinellas HMIS, regardless of whether the data has yet been entered into Pinellas HMIS, will be treated in the following manner:

1. Records shall be kept in individual locked files or in rooms that are locked when not in use.
2. When in use, records shall be maintained in such a manner as to prevent exposure of PII to anyone other than the user directly utilizing the record.
3. Employees shall not remove records or other information from their places of business without permission from appropriate supervisory staff unless the employee is performing a function which requires the use of such records outside of the MA's place of business and where return of the records by the close of business of would result in the undue burden on staff.
4. When staff remove records from their places of business, the records shall be maintained in a secure location and staff must not re-disclose the PII contained in those records except as permitted by these policies and procedures.
5. Faxes or other printed documents containing PII shall not be left unattended.
6. Fax machines and printers shall be kept in secure areas.
7. When faxing PII, the recipients should be called in advance to ensure the fax is properly managed upon receipt.
8. When finished faxing, copying, or printing all documents containing PII should be removed from the machines promptly.

Database Integrity
The MA may not intentionally cause corruption of the Pinellas HMIS in any manner. Any unauthorized access or unauthorized modification to computer system information, or interference with normal system operations, will result in immediate suspension of Pinellas HMIS licenses held by the MA, and suspension of continued access to the Pinellas HMIS by the MA.

Disaster Recovery
Pinellas HMIS data is stored by Mediware Information Systems in a secure and protected off-site location with duplicate back-up. In the event of disaster, the Pinellas HMIS System Administrator will coordinate with Mediware Information Systems to ensure the Pinellas HMIS is functional and that data is restored. The HLA will communicate to MA's when data becomes accessible following a disaster.

Contracts and other arrangements
The Pinellas HMIS Lead Agency shall retain copies of all contracts and agreements executed as part of the administration and management of the Pinellas HMIS or required to comply with HUD requirements for a five-year period.

Identification of Security Officer/Agency Administrator

Organization Name

Security Officer/Agency Administrator

Name Title Phone Email

Security Officer duties include, but are not limited to:

- ✓ Annually review the Security Certification document and test the Member Agency security practices for compliance.
- ✓ Using this Security Certification document, certify that the Member Agency adheres to the Security Plan or provide a plan for remediation of non-compliant systems, including milestones to demonstrate elimination of the shortfall over time. Communicate any security questions, requests, or security breaches to the Pinellas HMIS Director, System Administrator, and Security Officer.
- ✓ Communicate security-related Pinellas HMIS information to the organization's end users.
- ✓ Complete security training offered by the Pinellas HMIS Lead Agency.
- ✓ Additional duties specified in the Pinellas HMIS Participation Agreement.

Member Agency Security Officer signature indicating understanding and acceptance of these duties:

Signature _____ Date _____

Identification of Security Officer/Agency Administrator

Organization Name

Security Officer/Agency Administrator

Name Title Phone Email

Security Officer duties include, but are not limited to:

- ✓ Annually review the Security Certification document and test the Member Agency security practices for compliance.
- ✓ Using this Security Certification document, certify that the Member Agency adheres to the Security Plan or provide a plan for remediation of non-compliant systems, including milestones to demonstrate elimination of the shortfall over time. Communicate any security questions, requests, or security breaches to the Pinellas HMIS Director, System Administrator, and Security Officer.
- ✓ Communicate security-related Pinellas HMIS information to the organization's end users.
- ✓ Complete security training offered by the Pinellas HMIS Lead Agency.
- ✓ Additional duties specified in the Pinellas HMIS Participation Agreement.

Member Agency Security Officer signature indicating understanding and acceptance of these duties:

Signature _____ Date _____

Each Member Agency is required to meet the following security requirements. If the requirement cannot be met at the time of the initial certification, you must indicate a date not later than three months after the initial certification by which you will have met the requirement. At that time, you will be required to submit an updated version of this form demonstrating your compliance.

	Required policy	Meets Requirement (Yes/No)	If no, date by which compliance will be met
User Authentication	Does the agency abide by the Pinellas HMIS policies for unique user names and password?	All Pinellas HMIS users at the agency are aware that they should: NEVER share username and passwords ___Y___N NEVER keep usernames/ passwords in public locations ___Y___N NEVER use their internet browser to store passwords ___Y___N All users have signed a receipt of compliance for staff ___Y___N	
Hard Copy Data	Does agency have procedures in place to protect hard copy Personal Identifiable Information (PII) generated from or for the Pinellas HMIS?	Agency has procedure for hard copy PII that includes: (1) Security of hard copy files ___Y___N Locked drawer/file cabinet ___Y___N Locked office ___Y___N (2) Procedure for client data generated from the Pinellas HMIS Printed screen shots_____Y_____N HMIS client reports__Y_____N Downloaded data into Excel Y_____N Copy of above procedures is available ___Y___N Agency trains all staff on hard copy procedures___Y_____N	
PII Storage	Does the agency dispose of or remove identifiers from a client record after a specified period of time? (Minimum standard: 7 years after PII was last changed if record is not in current use.)	Agency has a procedure ___Y___N Describe procedure:	

Virus Protection	Do all computers have virus protection with automatic update? (This includes non-Pinellas HMIS computers if they are networked with Pinellas HMIS computers.)	Virus software and version _____ Auto-update turned on ___Y___N Date last updated:__/____/ _____ Person responsible for monitoring/updating:	
Firewall	Does the agency have a firewall on the network and/or workstation(s) to protect the Pinellas HMIS systems from outside intrusion?	Single computer agencies: ___Y___N Individual workstation ~~Version: _____~~ Networked (multiple computer) agencies: ___Y___N Network firewall Version: _____	
Physical Access	Are all Pinellas HMIS workstations in secure locations or are they manned at all times if they are in publicly accessible locations? (This includes non-Pinellas HMIS computers if they are networked with Pinellas HMIS computers.)	All workstations are: In secure locations (locked offices) or manned at all times ___Y___N Using password protected screensavers ___Y___N All printers used to print hard copies from the Pinellas HMIS are: In secure locations__Y____N Data Access: Users may access Pinellas HMIS from outside the workplace ___Y___N If yes, Agency has a data access policy Y____N	
Data Disposal	Does the agency have policies and procedures to dispose of hard copy PII or electronic media?	Agency shreds all hardcopy PII before disposal____Y____N Before disposal, the Agency reformats/degausses (demagnetizes): Disks__Y___N CDs___Y___N CDs Computer hard-drives____Y____N Other media (tapes, jump drives, etc.) ___Y___N	

Software Security	Do all Pinellas HMIS workstations have current operating system and internet browser security? (This includes non-Pinellas HMIS computers if networked with Pinellas HMIS computers.)	Operating System (OS) Version: _____ All OS updates are installed_Y____N Most recent version of Internet browser(s) are installed___Y____N	

We affirm and certify the above information is true and that this Member Agency, _____, is in full compliance with all requirements listed as "CHO" (Contributing HMIS Organization) responsibilities in the U.S. Department of Housing and Urban Development Homeless Management Information System (HMIS) Data and Technical Standards Final Notice and with the Pinellas County HMIS Policies and Procedures or will comply within the timeframes stated above. This certification is incorporated into the Pinellas HMIS Participation Agreement. Any misrepresentation of the foregoing may result in termination of the Participation Agreement.

_____ _____

Pinellas HMIS Security Contact Signature Date

_____ _____

Executing Officer Signature Date

Privacy Plan

Each Pinellas HMIS MA must have a Privacy Statement that describes how and when the MA may use and disclose clients' Private Personal Information (PPI). PPI includes name, Social Security Number (SSN), date of birth, zip code, project entry and exit, unique personal identification number (HMIS number) and project identification number.

MA's may be required to collect some PPI by law or may be required to collect data as a funding requirement. PPI is also collected by MA's to monitor project operations, to better understand the needs of people experiencing homelessness, and to improve services for people experiencing homelessness. MA's are only permitted to collect PPI only with a client's written consent.

MA's may use and disclose client PPI to:

1. Verify eligibility for services,
2. Provide clients with and/or refer clients to services that meet their needs,
3. Manage and evaluate the performance of programs,
4. Report about program operations and outcomes to funders and/or apply for additional funding to support agency programs,
1. Collaborate with other local agencies to improve service coordination, reduce gaps in services, and develop community-wide strategic plans to address basic human needs, and
5. Participate in research projects to better understand the needs of people served.

MA's may also be required to disclose PPI for the following reasons:

1. When the law requires it;
2. When necessary to prevent or respond to a serious and imminent threat to health or safety; and
3. When a judge, law enforcement or administrative agency orders it, MA's are obligated to limit disclosures of PPI to the minimum necessary to accomplish the purpose of the disclosure.

Uses and disclosures of PPI not described above may only be made with a client's written consent. Clients have the right to revoke consent at any time by submitting a request in writing. Clients also have the right to request in writing:

1. A copy of all PPI collected,
2. An amendment to any PPI used to make decisions about your care and services (this request may be denied at the discretion of the agency, but the client's request should be noted in the project records),
3. An account of all disclosures of client PPI,
4. Restrictions on the type of information disclosed to outside partners, and
5. A current copy of the MA's privacy statement.

All individuals with access to PPI are required to complete formal training in privacy requirements at least annually. MA Privacy Statements may be amended at any time. Amendments may affect information obtained by the agency before the date of the change. An amendment to the Privacy Statement regarding use or disclosure will be effective with respect to information processed before the amendment, unless otherwise stated. A record of all amendments to this Privacy Statement must be made available to clients upon request. This document should, at a minimum, reflect the baseline requirements listed in the HMIS Data and Technical Standards Final Notice, published by HUD in July 2004 and revised in March 2010. In any instance where this Privacy Statement is not consistent with the HUD Standards, the HUD Standards take precedence. Should any inconsistencies be identified, please immediately notify the Pinellas HMIS Lead Agency.

Pinellas Continuum of Care

Ending Homelessness Together

Pinellas Homeless Management Information System (HMIS) 2024 Data Quality Plan

TABLE OF CONTENTS

PURPOSE

This document describes the Homeless Management Information System (Pinellas HMIS) Data Quality Plan for Pinellas County. Adapted by a Plan developed from the Texas Balance of State Continuum of Care (CoC); it includes assurances and controls to maintain high data quality that meet requirements set forth by the U.S. Department of Housing and Urban Development (HUD) and responsibilities shared with the Homeless Leadership Alliance of Pinellas (HLA).

This Plan is to be updated annually, using the latest HUD HMIS Data Standards and CoC performance objectives.

BACKGROUND

Pinellas HMIS is a locally administered, electronic data collection system that stores longitudinal client-level information about the people who access homeless and housing services in the community. Each Continuum of Care (CoC) receiving HUD funding is required to implement HMIS to capture standardized data about everyone accessing the Homeless Crisis Response System. Furthermore, elements of HUD's annual CoC funding competition are directly related to a CoC's progress in implementing its HMIS.

Each and every Pinellas HMIS end user contributes significantly to the CoC. One project or one Pinellas HMIS end user with poor data quality can negatively impact the entire system.

HMIS data reported to federal funders provides estimates of the current state of homelessness across the country, and how the use of homeless assistance programs is reported to Congress. HMIS is used locally to inform state and local communities on how their specific homeless projects are performing and how information compares nationally. This also helps local communities to better allocate resources, and position programs to end homelessness.

The CoC's Data and System Performance Committee will recognize, quarterly, the work of providers meeting a high level of data quality to ensure Pinellas HMIS data quality is understood and applied. The CoC will work with local funders to also use data quality metrics when making funding allocation decisions to projects. The CoC will encourage local funders to include data quality within funding contracts and agreements with providers. The CoC will work with the Pinellas HMIS team and providers who do not currently use Pinellas HMIS to encourage data entry into Pinellas HMIS.

The CoC will work with Pinellas HMIS to monitor data quality at the end-user, project, agency, and system level. Data quality enforcements will depend on where data quality issues lie and could include:

- Locking specific providers or end-users out of Pinellas HMIS until they receive remedial or additional training from Pinellas HMIS.
- Remove the ability of a given end-user to access and enter data into Pinellas HMIS if data quality becomes a consistent issue that is not acknowledged or addressed.

UNIVERSAL DATA ELEMENTS

The data entered into Pinellas HMIS tells a story about the population experiencing homelessness. To end homelessness, the scope of the issue must first be recognized. How big is the problem, where is it hitting the most, what kind of projects are required. These questions and many more get answered thanks to the information collected and entered into Pinellas HMIS.

As of the 2018 Fiscal Year, HUD discontinued the use of the Annual Homeless Assessment Report (AHAR) data submission from HMIS in favor of the new Longitudinal System Analysis (LSA) report. The LSA reflects a major change in how annual HMIS client, project, and system level data is submitted to HUD. The LSA greatly expands the scope of the data submission, updates measures and categories to match current HUD parameters, aligns the submission with other HUD reporting, and puts a greater emphasis on the quality of a system's data when determining the usability of a submission when compared to the previous AHAR submission. Data contained within a CoC's LSA submission is included in the Annual Homeless Assessment Report (AHAR) that is written by HUD and submitted to Congress on an annual basis and may be considered for a CoC's annual HUD renewal funding through the Notice of Funding Availability (NOFA) process.

Universal Data Elements (REQUIRED)

Universal Data Elements (UDEs) for projects participating in HMIS:

3.01 Name
3.02 Social Security Number
3.03 Date of Birth
3.04 Race and Ethnicity
3.06 Gender
3.07 Veteran Status
3.08 Disabling Condition
3.10 Project Start Date
3.11 Project Exit Date
3.12 Destination
3.15 Relationship to Head of Household
3.16 Enrollment CoC
3.20 Housing Move-in Date

Unless otherwise determined, the HUD UDEs are the minimum required data elements that must be collected and entered into Pinellas HMIS by participating agencies. The various federal partners (Health and Human Services, Veterans Affairs, etc) provide detailed instructions to grant recipients and require the collection of certain Program Specific Data Elements (PSDEs) by funded projects, as established in the HUD Data Standards and the respective federal partner HMIS project manuals. Other funders (local, state, etc) may also require the collection of existing PSDEs or other custom data elements by funded projects for reporting, eligibility, and benchmark purposes.

PROGRAM SPECIFIC DATA ELEMENTS (PSDEs)

Unlike UDEs, the Program Specific Data Elements are specialized for each Federal/State/local funding partner and their programs. A partner may require all of the fields or response categories in a data element or may specify which of the fields or response categories are required for their report. The list below are examples of required PSDEs by Federal Partners (see Data Standards or individual Program Manuals):

4.02 Income and Sources
4.03 Non-Cash Benefits

4.04 Health Insurance
4.05 Physical Disability
4.06 Developmental Disability
4.07 Chronic Health Condition
4.08 HIV/AIDS
4.09 Mental Health Disorder
4.10 Substance Use Disorder
4.11 Domestic Violence
4.12 Current Living Situation
4.13 Date of Engagement
4.14 Bed-Night Date
4.19 Coordinated Entry Assessment
4.20 Coordinated Entry Event

DATA QUALITY PLAN

This Plan focuses on the reliability and validity of client-level data collected in the HMIS. It is measured by the extent to which the UDEs entered in the system reflects actual information in the real world. With good data quality, the CoC can tell an accurate story about the population experiencing homelessness.

The Plan defines conditions, assigns responsibilities, and establishes standard procedures to maintain and/or improve quality. As a result, a data quality plan can better position the CoC to achieve strategic objectives. This is a collaboration between projects, funding partners, HMIS, and the CoC. The plan specifies metrics for relevant and measurable attributes utilized to assess data quality: **timeliness, completeness, accuracy, and consistency**.

Timeliness

Timeliness is closely associated with relevance and prevents duplication of services. If the data entry is delayed, the data may no longer be relevant for the needs of end users. Timely data entry reduces human error (relying on handwritten notes or memory) and ensures better management, either proactively (monitoring, increasing awareness, meeting funder requirements), or reactively (requests for information, responding to inaccurate information).

While every effort should be made to complete all data entry in electronic records at the time of service there are occasional circumstances that prevent that goal. To comply with reasonable quality standards, HMIS establishes the following policy regarding client record data entry:

- All HMIS Member Agency client data should be entered no later than 72 hours after intake, assessment, or program or service entry or exit. In the event Pinellas HMIS end users are not able to enter data in real time, the project entry date needs to be the date the actual service begins and **not** the date of data entry.

The HMIS staff will assess timeliness monthly, the HLA's Data and System Performance Committee quarterly.

Completeness

Complete HMIS data is required to fully understand the demographic characteristics and service use of clients in the Homeless Crisis Response System. It is also crucial to assist clients in finding the right services, projects and/or benefits to end their homelessness experience as quickly as possible.

Complete data facilitates accurate reporting and analysis on the nature and extent of homelessness, such as:

- Unduplicated counts of clients served locally
- Patterns of use of people entering and exiting the Homeless Crisis Response System
- Estimation of the effectiveness of the CoC Homeless Crisis Response System

Projects are required to enter 100% of the clients served into HMIS after consent has been provided by the client*

Missing data negatively affects the ability to provide comprehensive care to clients. Eligibility determination, for instance, is directly tied to the data provided. Therefore, all participants agree, upon HMIS implementation, to adopt and enforce intake and assessment procedures that align with data collection requirements to prevent incomplete data.

While the CoC's goal is to collect 100% of all data elements, this may not be possible in all cases. While "client doesn't know" and "client refused" are eligible responses to individual client intake and assessment questions, the CoC defines acceptable rates for total "unknown" responses at the program level based on data element and project type considerations.

***Use of Verbal Consent**
While a signed Pinellas HMIS Informed Consent and Release of Information form is preferred, agencies may be allowed to utilize verbal consent based on the nature of the project or if a state of emergency is declared. Refer to the Pinellas HMIS Policies and Procedures for more information.

HMIS will review completeness of data monthly, HLA's Data and System Performance Committee quarterly.

Accuracy

The data in HMIS needs to exhibit a fair representation of reality as it relates to homeless clients and the projects that serve them. Thus, all data entered into HMIS must be a reflection of information provided by the client, as documented by the data collector or otherwise updated verbally by the client and documented for reference.

Recording inaccurate information is strictly prohibited. Organizations need to make every effort to record accurate data by implementing appropriate policies and procedures. The best way to measure accuracy of client data is to **verify** the information with more accurate sources, such as a social security card, birth certificate, or driver's license.

False or inaccurate information is less useful than incomplete information. It should be emphasized to clients and staff that it is better to enter "Client Doesn't Know", "Client Prefers Not to Answer" or "Data Not Collected", than to enter inaccurate information.

HMIS reviews accuracy monthly through multiple system and project-level reports such as the System Performance Measures, Monthly Data Dashboards, and Benchmark Reports.

Consistency

Consistency refers to the standard and uniform practice for implementation, data collection and data entry across all programs in HMIS. Inconsistency hinders an agency's ability to satisfy requirements as they relate to timeliness, completeness and accuracy.

To ensure quality, all prospective projects will implement HMIS, e.g., intake and assessment forms, eligibility requirements; and comply with the recommendations of HMIS consistent with best practice.

The HLA may delay or cancel implementation if the agency does not consistently participate in the process. Upon implementation, all HMIS users shall complete training before they may access HMIS and are required to attend annual training.

Consistency will be regularly monitored by HMIS. HMIS staff reviews and merges duplicated client records on a weekly basis, this also includes duplicate entries/exits. To resolve duplication, projects may need to provide additional information to HMIS in order to properly identify clients with incomplete data and rule out any false positives.

When first identified, records are audited to determine cause of duplication. Duplicative client records are merged by HMIS and any duplicative entry/exits are also removed A technical assistance reminder of HMIS best practices will be sent out to the end user; however, if duplication persists, the end user in question must participate in additional training from HMIS and their Agency Administrator will be notified.

Bed Utilization

For shelters and housing projects, one of the primary features of HMIS is its ability to record the number of client stays or bed nights in a housing project. A housing project's bed utilization rate is the number of beds occupied as a percentage of the entire bed inventory. The client must be checked into a bed or unit in HMIS. The client remains in that bed or unit until they are transferred to another bed or unit, or exited from the project.

A project's bed utilization rate is a great indicator of data quality. A low utilization rate could reflect low occupancy, but it could also indicate that data is not being properly entered in HMIS for every client served. A high utilization rate could reflect that the program is over capacity, but it could also indicate that clients have not been properly discharged from the program in HMIS.

Housing Program Type	Target Utilization Rate (%)	Acceptable Rate (%)
Emergency Shelter	**75%**	**65%**
Transitional Housing	**95%**	**85%**
Permanent Supportive	**95%**	**85%**
Safe Haven	**95%**	**85%**

Zip Code Data Entry into Pinellas HMIS
The Pinellas Continuum of Care is dedicated to making data-driven decisions that use a racial equity framework. In response to the growing housing availability crisis, the CoC needs to track and report where affordable and safe housing is being secured to rehouse households coming into the Homeless Crisis Prevention and Response System. This data will allow the CoC to identify geographic housing gaps to demonstrate how potential funding restrictions may be causing barriers to housing.

Zip code is required for:

- Homeless Prevention and Diversion services enter Pinellas HMIS, zip code data for all project participants. Zip codes are to be added under "Client's Information/Last Permanent Address."
- Permanent Housing and Permanent Supportive Housing, including Rapid Re-Housing providers, are to enter zip code data into the "Zip Code" field next to the "Housing Move-in Date."

Emergency Shelters, Safe Havens, Street Outreach, and Transitional Housing projects are encouraged to collect zip code data under "Client's Information/Last Permanent Address." However, zip code data is not a required field to be completed these projects.

PROVIDER ACCOUNTABILITY

Agency Administrators are required to submit certification to Pinellas HMIS stating the Data Quality Reports were reviewed, and any identified errors were corrected by their agency end users by the 7th of each month. The Pinellas HMIS staff will then run and review the reports to ensure data quality, for all projects.

1. If an error rating rises above the target percentage for a project, HLA will create a Training Plan of Action for the HMIS end user(s).
2. If the error rating for the project remains above the acceptable target error percentage for three months, HLA may implement a Training Plan and/or Corrective Action Plan, which would be monitored by the Data System and Performance Committee. The course of action taken, whether training or corrective action, will be handled on a case-by-case basis.
3. If an Agency is found to be non-compliant with a Training Plan and/or Corrective Action Plan, or if there are repeated data quality errors, the agency could be jeopardizing their project(s) funding and/or the CoC's funding, therefore the Agency would be brought to the HMIS Governance Committee to determine continuation of HMIS access and licensing status.

HLA staff will communicate with project managers, as well as organizational executive staff, as to the status of a project's training plan and potential need for corrective action due to on-going data quality concerns. A training plan consists of, but may not be limited to, supporting end users and agency administrators with the training, knowledge, reporting, and support needed to collect, enter, and maintain accurate data in the Homeless Management Information System software. **Pinellas HMIS reserves the right to request any HMIS end user to be re-trained. Non-compliance with the training request will revoke all login credentials.**

Data Quality Reports—Report names TBD based on updates to the Reporting tools available

The report for timeliness measures the difference between the date stamp on the Program Entry or Service Date displayed in Pinellas HMIS to the actual system date stamp that is recorded hen an end-user created the Project Entry or Service in the system. Data quality for timeliness is used to monitor the CoC benchmark for Timeliness (see page 3). The report for data completeness provides a measure of how complete the local CoC Data Quality Benchmarks are based on project type. The Data Quality Benchmarks are found below.

The reports used for certification may be a combination of vendor-created and locally-created reports. The specific report names are subject to change based on updates to the Reporting tools available or based on local need. Changes will be communicated to Agencies at least thirty (30) days prior to the change going live and relevant report training will be provided to Agency Administrators.

CONTINUUM OF CARE (CoC) REPORTS

Below are reports the HLA staff and Data and System Performance Committee utilizes when reviewing system performance and data quality.

Local Reports	Report Frequency	Data Source
CoC System Dashboard	Monthly	HMIS
USICH Veteran Benchmarks	Monthly	HMIS
CoC Performance Dashboard	Quarterly	HMIS
CoC Project Benchmarks	Quarterly	HMIS
System Performance Measures (SPMs)	Annually	HMIS
Annual Performance Reports (APR)	Annually	HMIS
Longitudinal System Analysis (LSA)	Annually	Stella P
Housing Inventory Count (HIC)	Annually	HMIS
Point-in-Time Count	Annually	HMIS (Sheltered count) Street Surveys (Unsheltered Count)

COC DATA QUALITY BENCHMARKS
Approved by the Data and System Performance Committee January 12, 2024

All UDE's must be obtained from each adult and unaccompanied youth who apply for services through the homeless assistance system. Most UDEs are also required for children aged 17 years and under.							
The target for all Data Elements is 100%. The acceptable Null/Missing target is 0%.							
Universal Data Element	**Permanent Housing (includes Permanent Supportive Housing, Rapid Rehousing)**	**Transitional Housing**	**Supportive Services Only**	**Emergency Shelter (Includes Family Bridge Housing)**	**Homeless Prevention**	**Coordinated Entry**	**Street Outreach**
	Unacceptable "Client Doesn't Know", Client Prefers not to Answer"						
Name	0%	0%	0%	0%	0%	0%	10%
Social Security Number	5%	5%	5%	10%	5%	5%	50%
Date of Birth	1%	1%	1%	2%	1%	1%	10%
Race	1%	1%	1%	5%	1%	1%	10%
Gender	1%	1%	1%	1%	1%	1%	10%
Veteran Status	1%	1%	1%	1%	1%	1%	10%
Disabling Condition	1%	1%	1%	1%	1%	1%	10%
Exit Destination	2%	2%	2%	30%	2%	30%	30%
Relationship to Head of Household	0%	0%	0%	0%	0%	0%	0%
Client Location (Enrollment CoC)	0%	0%	0%	0%	0%	0%	0%
Housing Move-in Date	0%						
Prior Living Situation	0%	0%	0%	0%	0%	0%	0%
Length of Stay in Previous Place	0%	0%	0%	5%	0%	0%	10%
Approximate Date Homelessness Started	0%	0%	0%	5%	0%	0%	10%
Number of Times Homeless	0%	0%	0%	5%	0%	0%	10%
Number of Months Homeless	0%	0%	0%	5%	0%	0%	10%

Pinellas County Continuum of Care Data Quality Roles and Responsibilities

The different roles associated with HMIS data collection, operations, policy and procedure development, and DQ monitoring and reporting can all play a meaningful part upholding a CoC's Data Quality Management Program.

Data Collection and Entry

Role	Responsibility
Collect HUD assessment data from clients	Agency Projects
Enter HUD entry assessment data in HMIS	Agency Projects
Update HMIS to reflect change in income, benefits, etc.	Agency Projects
Collect HUD exit assessment data from clients (including exit destination)	Agency Projects
Enter HUD exit assessment data in HMIS	Agency Projects
Dismiss clients from programs in HMIS	Agency Projects
Make or change a bed/unit reservation for a client	Agency Projects
Notify HMIS to merge identified duplicate clients across the HMIS	Agency Projects
Secure paper forms according to privacy and confidentiality standards	Agency Projects
Maintain workstation security	Agency Projects

HMIS Operations

Role	Responsibility
Develop and deliver training for new end users	HMIS Lead Agency
Provide annual refresher training to end users	HMIS Lead Agency
Develop and deliver training for medium to advanced-level users	HMIS Lead Agency
Maintain documentation of completed training requirements	HMIS Lead Agency
Authorize/provide HMIS access or licenses to new end users	HMIS Lead Agency
Remove HMIS access or licenses due to violation or end of employment at the HMIS-participating agency	HMIS Lead Agency
Review HMIS data standards updates for correctness and completeness	HMIS Lead Agency
Manage project set up tasks	HMIS Lead Agency
Provide troubleshooting/technical assistance via service help desk activities	HMIS Lead Agency
Solicit feedback from HMIS stakeholders on HMIS policies and operations	HMIS Lead Agency
Provide communications about upcoming agency-specific HMIS changes	HMIS Lead Agency
Provide communications about CoC-wide or HUD-mandated HMIS changes	HMIS Lead Agency

Document workflow needs by program	HMIS Lead Agency
Implement program-level workflow, features, and functionality	HMIS Lead Agency
Monitor the HMIS vendor against the terms and conditions of the contract	HMIS Lead Agency
Update and revise the HMIS vendor contract	HMIS Lead Agency
Review HMIS software functionality updates for correctness and accuracy	HMIS Lead Agency
Test new features and functionality	HMIS Lead Agency

Policies and Procedures

Role	Responsibility
Develop data quality plans, policies, and procedures, including DQ benchmarks for timeliness, completeness, accuracy, and consistency	HMIS Lead Agency, CoC Lead Agency, and DSP Committee
Approve data quality plans, policies, and procedures, including DQ benchmarks for timeliness, completeness, accuracy, and consistency	HMIS Governance
Review data quality plans, policies, and procedures for appropriateness in relation to CoC's needs	DSP Committee
Implement DQ plans, policies, and procedures	CoC Board of Directors
Conduct monitoring and oversight of end users to ensure HMIS activities are implemented with fidelity to approved plans, policies, and procedures	HMIS and CoC Lead Agency(s)
Develop program- and user-level forms and documents (such as HMIS end user agreement or client releases of information)	HMIS Lead Agency
Define roles and responsibilities of HMIS end users	HUD
Define roles and responsibilities of the HMIS decision-making entity across the CoC (e.g., executive board, designated committee, or work group)	HMIS Governance
Define roles and responsibilities of HMIS Lead	HUD
Review and approve HMIS data requests for external research/evaluation projects	DSP Committee
Provide HMIS data to external researchers/evaluators	HMIS Lead Agency
Participate in the HMIS Work Group (Would also include training needs)	DSP Committee

Monitoring and Reporting

Role	Responsibility
Monitors data quality for completeness (client and program)	HMIS and CoC Lead Agency(s)
Monitor data quality for timeliness	HMIS and CoC Lead Agency(s)
Monitor data quality for accuracy	HMIS and CoC Lead Agency(s)
Monitor data quality for consistency	HMIS and CoC Lead Agency(s)
Analyze project-level and system-level trends in DQ performance	HMIS and CoC Lead Agency(s)
Running data quality/validation reports	HMIS Lead Agency and Provider Agency Administrators
Correct low quality data across the HMIS implementation	Provider Agency Administrators and HMIS Lead Agency
Correct low quality data at the program level	Provider Agency Administrators and HMIS Lead Agency
Communicate low data quality performance to appropriate stakeholders (e.g., discussing improvement strategies with agencies or elevating issues up to DQ enforcement entity/CoC when necessary)	HMIS and CoC Lead Agency(s)
Communicate high data quality performance to appropriate stakeholders (e.g., public recognition)	HMIS and CoC Lead Agency(s)
Evaluate current DQ monitoring processes and identify new protocols for continuous improvement	HMIS and CoC Lead Agency(s)
Evaluate current DQ incentives and enforcements and identify new resources for continuous improvement	HMIS and CoC Lead Agency(s)
Review HUD reports prior to submission	HMIS and CoC Lead Agency(s)
Submit HUD reports in Sage or HDX	HMIS and CoC Lead Agency(s)
Manage program-level reporting requirements by service and/or funder	CoC Lead Agency
Conduct Point in Time Count reports as required by the CoC	HMIS and CoC Lead Agency(s)
Provide Housing Inventory reports to the CoC	HMIS and CoC Lead Agency(s)
Develop and review data dashboards/visualizations, if applicable	HMIS and CoC Lead Agency(s)

List of Revisions, Additions, and Deletions to Pinellas HMIS Data Quality Plan

1. Version One 10/02/2019
2. Version Two 2/12/2019
3. Reviewed 03/2021
4. Updated 02/18/2022
5. Annual Review 02/07/2023
6. Updated Benchmarks 02/08/2024