Pinellas County Homeless Leadership Board
Data and System Performance Committee Meeting
June 13, 2019 9:30 a.m. – 11:00 a.m.
Location: Service Source

UPDATED AGENDA

1. Approval of May Minutes             Action Item

2. Data Review:                          Action Item
   a. Monthly Data
   b. Veteran Data
   c. Pinellas HMIS Qlik Sense Preview

3. Update Regarding HLB Request for Future Funding Prioritization   Information Item

4. School Data Follow-Up                Information Item
   The residency questionnaire would be completed during the school year when a family reports a new address to screen if the new living situation meets McKinney Vento criteria and anytime a student to enrolls at a school during the school year. HEAT team and school staff complete the form.

   Quarter I Pinellas County Schools homeless student data, broken out by schools is not broken out by month.

5. HMIS Policies and Procedures Annual Review   Action Item
   a. Law Enforcement Policy
   b. Review HMIS Access Request Form

6. System Performance Measures          Action Item

7. Update from Racial Disparities Subcommittee Information Item

8. Review July Agenda                   Discussion Item
   a. CoC Benchmarks
Attendees:
Stephanie Reed          Brian Leaply
Ricky Zanker           Avery Slyker
Marina Pantuso         Cindy Kazawitch
Jodi Seitanakis
David Laake
Sam Picard
John Morgan
Jume Valdez
Shelia Lopez
Christa Bruning
Kevin Marrone
Corey Recvolohoe

1. Agenda Item: Minutes from March 2019
Marina Pantuso moved to accept the minutes, Ricky Zanker seconded; Motion passed.

2. Agenda Item: PHMIS View Only Process
HMIS staff to create a form for organizations requesting entry into HMIS system. This form needs to include baseline criteria of what is required from organizations to enter the system, including costs. The form will also contain information about whether data will be shared internally with non-HMIS users.

3. Agenda Item: Data Review
The committee approved of the new report formatting and agreed to leave the “missed curfew” data within the exit information, as it shows the progress HMIS staff is having with their training and it shows the reality of what is happening within the Crisis Response System. The chair would like the CoC to advocate to HUD, changes to the Return to Homelessness System Performance Measure report. The CoC can only extract Permanent Supportive Housing data by project under “exits from PH,” annually. The data that the HLB receives monthly regarding “exits from PH” include PSH, VASH, PH, Shelter+Care and HOME Voucher Program. HLB staff suggested the committee forward this concern to the Strategic Planning Committee.

The committee reviewed the quarter two data from Pinellas County School’s HEAT Team, to prepare a presentation to the HLB’s June meeting. The committee agreed to share the raw data with the HLB but not any analysis of the data, including the GeoMap. The HLB presentation needs to stress; there is no way for the HLB staff or the committee to compare HEAT data to Pinellas HMIS data. One of the primary concerns of the committee is that there may be multiple counts of homelessness per student (i.e., began school year in hotel then moved to shelter in October or visa versa). Additionally, per Ray Santa Lucia, the HEAT data is cumulative, meaning the data is showing the increase of homeless students over the school year. The committee would like to ask the HLB how to proceed. One option would be to focus on the August 2018 data.
Stephanie Reed moved to approve the data reports and school data presentation; Shelia Lopez seconded; Motion passed.

4. Agenda Item: VA Training
HMIS staff provided training on the VA benchmark data. The training included how HMIS pulls the data for the report. HMIS staff stated for the CoC to meet all the VA benchmarks, it will need data from outside of HMIS. It was clarified for the committee that Benchmark B is the first time a client touches the Homeless Crisis Response System but if the individual disappears for 90+ days when they return to the system, the first-time count begins again for the individual. Currently, the benchmarks are seeing fluctuation due to the number of individuals that have been homeless for hundreds of days being housed.

5. Agenda Item: HLB Request
During the April 2019 HLB meeting, a motion was approved to request the DSP committee review and define a proposal to bring forward to the HLB for approval on how the prioritization will be set for both HUD and other funding for the CoC for the future. Additionally, the HLB would like to know how the committee would consider the HEAT data and how to incorporate this data into prioritization best. The committee stated there should be a designated committee meeting to discuss that includes looking at the past NOFA scores to see why we have lost points. Additionally, the discussion should include how to incorporate vulnerability. The committee will then forward to the DSP Review and Rank Subcommittee to create a proposal to send to the HLB.

Agenda Item Update: Per HLB Executive Staff, there are funded agencies that sit on the DSP Committee therefore; the full DSP Committee should not discuss this issue, as there could be perceived bias. This item is to be forwarded to the DSP Review and Rank Subcommittee.

John Morgan moved to extend the committee meeting to 11:30 a.m.

6. Agenda Item: CoC Benchmarks
The chair opened the discussion by stating there is a disconnect from benchmark to the actual measures for Benchmark A. Performance needs added so that this data can be compared month to month. The committee also recommended using the Veteran Trend Data Report as the template for how to report on the CoC Benchmarks. HLB staff pointed out to the committee that adding the suggested performance measures to Benchmark A would replicate the SPM. The committee asked why the CoC couldn’t just adopt the SPM as the system benchmarks. HLB staff reviewed with the committee, recommended best practices from HUD and CoC’s nationwide, pointing out that CoC’s should be implementing their own, system-specific benchmarks. The committee stated they would spend the June committee meeting reviewing the Ohio BoSCoC Benchmarks.
Entries

**Monthly Housing Placement Rate: 26%**

Housing Placement Rate = Total Unduplicated Positive Exits (310) / Total Unduplicated Number of Clients (1,211)

Unduplicated Individuals that Entered the Homeless Crisis Response System

There were a total of 1,304 unduplicated exits for May 2019.

Exit Destinations

There were an additional 1,976 active, unduplicated clients carried over from April 2019.

Exits

310 individuals (unduplicated) had positive exits during May 2019.

There were a total of 1,304 unduplicated exits for May 2019.

Unduplicated Individuals that Exit the Homeless Crisis Response System

Total Clients - Unduplicated

Percentage of Clients
### Individuals Who Returned to Homelessness

**34.3%** May 2019 Total Returns to Homelessness in Two Years  
**31%** FY 2018 Total Returns to Homelessness in Two Years

**Measure 2a and 2b: The extent to which Persons who Exit Homelessness to Permanent Housing Destinations Return to Homelessness within 6 to 12 months (and 24 months in a separate calculation)**

<table>
<thead>
<tr>
<th>Project Type</th>
<th>Total # of Persons whoExited to Permanent Housing Destination (2 Years Prior)</th>
<th>Returns to Homelessness in less than 6 Months (0-180 days)</th>
<th>ONLY Returns to Homelessness from 6 to 12 Months (0-360 Days)</th>
<th>Cumulative Returns to Homelessness from 21 to 24 Months (0-365 Days)</th>
<th>ONLY Returns to Homelessness from 13 to 24 Months (0-730 days)</th>
<th>Cumulative Returns to Homelessness from 0 to 24 Months (0-730 days)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exit was from ES</td>
<td>2221</td>
<td>572</td>
<td>25.75%</td>
<td>168</td>
<td>740</td>
<td>33.32%</td>
</tr>
<tr>
<td>Exit was from TH</td>
<td>408</td>
<td>53</td>
<td>12.99%</td>
<td>27</td>
<td>80</td>
<td>19.61%</td>
</tr>
<tr>
<td>Exit was from SH</td>
<td>44</td>
<td>4</td>
<td>9.09%</td>
<td>3</td>
<td>7</td>
<td>15.91%</td>
</tr>
<tr>
<td>Exit was from PSH</td>
<td>116</td>
<td>7</td>
<td>6.03%</td>
<td>5</td>
<td>12</td>
<td>10.34%</td>
</tr>
<tr>
<td>Exit was from RRH</td>
<td>476</td>
<td>29</td>
<td>6.09%</td>
<td>18</td>
<td>47</td>
<td>9.87%</td>
</tr>
<tr>
<td>TOTAL Returns to Homelessness</td>
<td>3265</td>
<td>665</td>
<td>20.37%</td>
<td>221</td>
<td>886</td>
<td>27.14%</td>
</tr>
</tbody>
</table>

Data obtained for this section of the May 2019 Data Dashboard is from the HUD Required, System Performance Measure, HMIS Report 0701, Measure 2a and 2b: The Extent to Which Persons Who Exit Homelessness to Permanent Housing Destinations Return to Homelessness within 24 months. HUD includes PSH, VASH, Shelter+Care, and HOME Voucher Program within the PSH Exits.

### May 2019 Race/Ethnicity

- **31.27%** of entries were Black or African American.  
- **7.34%** of entries were Hispanic/Latino.

### Pinellas HMIS Dashboard Report Definitions

- **Housing Placement Rate** - The number of individuals with positive exits during the month divided by total number of individuals that entered the Homeless Crisis Response System during the month.
- **Entries** - The point of entry into the Homeless Crisis Response System.
- **Individuals** - An unduplicated/duplicated (indicated) count of adults and children.
- **Project Type** - CoC program component (Permanent Supportive Housing, Rapid Re-Housing, Transitional Housing, Safe Haven, Emergency Shelter, and Prevention Services.)
- **System Performance Measures (SPM)** - Seven System Performance Measures to help communities gauge their progress toward the goal of ending homelessness. Each Continuum of Care (CoC) is expected to use these measures to evaluate how well homeless systems are functioning and where improvements are necessary. These two System Performance Improvement briefs highlight different aspects to help CoCs better understand and improve their homeless system.
- **Carried Forward** - Individuals that were enrolled in the Homeless Crisis Response System the month prior to the reporting period and remain open.
- **Exits** - Represents the end of an individual's participation within a project.
- **Positive Exits** - Individuals that moved into permanent destinations.
- **Negative Exits** - Individuals that have ended participation within a project but have not moved into permanent destinations.

Veteran Trend Report is based on information provided within the Pinellas Homeless Management Information System (Pinellas HMIS), as of June 10, 2019.

Note: Exempted groups one and two have not been applied to Benchmarks A or B:

Exempted Group 1: Those Veterans experiencing either chronic or long-term homelessness who have been identified and offered a permanent housing intervention within the last two weeks but who have not yet accepted. Communities are responsible for ensuring that these Veterans are continually engaged and receive a documented offer of permanent housing at least every 14 days.

Exempted Group 2: Those Veterans experiencing either chronic or long-term homelessness who have been offered an available permanent housing intervention but have declined and instead chosen to enter a transitional housing program in order to appropriately address a clinical need. Veterans who have chosen to enter transitional housing programs in order to access generalized case management or job training are not included within this exempted group. (Note: Federal agencies will not be asking for detailed or personalized information regarding such exemptions, such as official confirmation of clinical needs.)

Not Met - Benchmark A - Chronic and long-term homelessness among Veterans has been ended. PHMIS Data only.

The community has no Veterans experiencing chronic or long-term homelessness, with the rare exceptions of:

1. Any Veteran who has been identified and offered an available permanent housing intervention, but who has not yet accepted;
2. Any Veteran who has been offered an available permanent housing intervention but has declined and instead chosen to enter a transitional housing program in order to appropriately address a clinical need, such as by providing, for example, treatment and services for homeless Veterans with substance use disorders or other mental health disorders, Safe Haven-like services for chronically homeless Veterans, or recuperative care for homeless Veterans post hospitalization; and,
3. Any Veteran that has accepted a permanent housing intervention but is still actively in the process of identifying, securing, or moving into a unit. It is important to note that this exemption expires 90 days after acceptance of the permanent housing intervention. The community continues to outreach to any Veterans experiencing long-term homelessness that has not yet accepted an offer of a permanent housing intervention, and continues to offer an available permanent housing intervention to those Veterans at least once every two weeks.

(All three months must meet the criteria in order for the benchmark to have been met.)
Not Met - Benchmark B - Veterans have quick access to permanent housing. PHMIS Data only. The community has a system in place to connect Veterans experiencing homelessness to permanent housing in an average of 90 days or less, measured from the day they are identified as experiencing homelessness to the day they enter permanent housing.

Met - Benchmark C - The community has sufficient permanent housing capacity. The number of Veterans exiting homelessness and moving into permanent housing is greater than or equal to the number of Veterans entering homelessness.

Met - Benchmark D - The community is committed to Housing First and provides service-intensive transitional housing to Veterans experiencing homelessness only in limited instances. PHMIS Data only. The number of Veterans experiencing homelessness who enter service-intensive transitional housing is significantly less than the number of Veterans entering homelessness.

Data notes:
- The count for the Veterans that entered service-intensive Transitional Housing is continuous for the 90-day period of the report. This means, these individuals may have been housed at any time during the 3-month period.
- Newly Identified Homeless Veterans: These are individuals within the continuous 90-day period preceding the benchmark measurement.
Pinellas HMIS Policies and Procedures
Table of Contents

Table of Contents
Overview and Introduction
  Benefits of PHMIS
  Handbook Format
  Acknowledgements
  HUD HMIS Data and Technical Standards Final Notice
  Domestic Violence Shelters and Programs
Section 1: Contractual Requirements and Roles
  Policy 1.1: PHMIS Contract Requirements
  Policy 1.2: PHMIS Governance Committee
  Policy 1.3: PHMIS Management
  Policy 1.4: Member Agency Responsibility
  Policy 1.5: Member Agency Administrator
  Policy 1.6: User
  Policy 1.7: Training
  Policy 1.8: Amending Policies and Procedures
  Policy 1.9: Required Licensing Fees
  Policy 1.10: Subsidized Licensing
Section 2: Participation Requirements
  Policy 2.1: Participation and Implementation Requirements
  Policy 2.2: Data Security Responsibility
  Policy 2.5: Client Consent for Electronic Data Sharing
  Policy 2.6: Confidentiality
  Policy 2.7: Information Security Protocols
  Policy 2.8: Connectivity
  Policy 2.9: Maintenance of Onsite (Agency) Computer Equipment
  Policy 2.10: Universal Data Elements
  Policy 2.11: PHMIS Grievance
Section 3: User, Location, Physical, and Data Access
  Policy 3.1: Access Levels for System Users
  Policy 3.2: Access to Data
  Policy 3.3: Access to Client Paper Records
  Policy 3.4: Unique User ID and Password
  Policy 3.5: Right to Deny User and Member Agencies’ Access
  Policy 3.6: Data Access Control
  Policy 3.7: Using PHMIS Data for Research
Section 4: Data Quality and Monitoring
  Policy 4.1: PHMIS Data Quality Policy
  Policy 4.2: Quality Monitoring
Section 5: Technical Support and System Availability
  Policy 5.1: Technical Support
  Policy 5.2: PHMIS Staff Availability
Section 6: Training Information
Section 7: Attachments
OVERVIEW AND INTRODUCTION

These Policies and Procedures were developed to guide the operation of the Pinellas Homeless Management Information System (PHMIS). The PHMIS 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 Homeless Management Information System Governance Committee (PHMIS Governance Committee) oversees and guides the development and management of the PHMIS. The PHMIS Governance Committee is comprised of the executive committee of the Homeless Leadership Board. Through the direction of these dedicated PHMIS Governance Committee members, these Policies and Procedures reflect the community’s stance on the operation of the PHMIS. The Homeless Leadership Board is the administrating agency for PHMIS and convenes the PHMIS Governance Committee.

The PHMIS Governance Committee has as guiding principles that the PHMIS:

- Is an implementation which 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
- Uses a data security approach to information management 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.

An underlying philosophy that has driven the process is respect for the personal data of each individual. Clients must give informed consent to having their data entered into the system. They must also authorize the sharing of their data and specify with whom it may be shared. They may decide not to participate and they may not be denied services for lack of participation.

A goal of the PHMIS is to inform public policy makers about the extent and nature of homelessness in Pinellas County, Florida, as the HLB endorses the philosophy of Housing First and believes it will greatly assist in the goal of making homelessness rare, brief and nonrecurring for Pinellas County citizens. This is accomplished through analysis of data that is grounded in the actual experiences of homeless persons and the service providers who assist them in shelters and homeless assistance programs. Information is gathered via interviews conducted by service providers with consumers is 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. PHMIS regulates HMIS licenses for community stakeholders serving homeless persons, also known as covered homeless organizations (CHO). Many CHO’s do not receive CoC funding and participate in HMIS voluntarily. All CoC funded, contracted agencies are required to participate in HMIS.

The PHMIS utilizes web-based software from Mediware. Through this software, homeless service organizations across the Continuum of Care (CoC) are able to capture information about the clients they serve. PHMIS staff provides technology, training and technical assistance to users of the system throughout the region.
**BENEFITS OF PHMIS**

**For individuals and families:**
- A decrease in duplicative intake and assessments
- Streamlined referrals
- More coordinated case management
- 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:**
- Improved ability to track client outcomes
- Improved coordination of services, internally among agency programs and externally with other service providers
- Improved data used for preparing reports to funding entities, boards and other stakeholders and advocacy for additional resources
- Aggregate information that can be used in program design and implementation through a more complete understanding of clients’ needs and 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:**
- Understanding of the extent and scope of homelessness
- Unduplicated count of clients
- Identification of service gaps
- Utilization of aggregated information for system design
- Development of a forum for addressing community-wide issues
- Enable McKinney-Vento funded organizations to meet the congressional mandate specified in the HUD Data and Technical Standards Final Notice
- 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 nonrecurring
**HANDBOOK FORMAT**

This handbook contains the most current information on the operation of the PHMIS. It is expected that information will be added, removed and altered as necessary as the program evolves. 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 PHMIS Policy and Procedures Handbook draws heavily from 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 (2017, July):

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-administered data system used to record and analyze client, service, and housing data for individuals and families who are homeless or at risk of homelessness. HMIS is administered by the U.S. Department of Housing and Urban Development (HUD) through the Office of Special Needs Assistance Programs (SNAPS) as its 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 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 original standards served as the foundation for software developers in constructing HMIS applications. In March 2010, HUD updated the Data Standards (March 2010 HMIS Data Standards), primarily to reflect data collection requirements for the Homelessness Prevention and Rapid Rehousing Program (HPRP). HUD, in collaboration with its federal partners, updated the HMIS Data Standards again in 2014 with the release of the 2014 HMIS Data Standards Manual and Data Dictionary. Both documents superseded the previously released HMIS Data Standards.
DOMESTIC VIOLENCE SHELTERS AND PROGRAMS

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

If an organization's primary mission is other than those listed above, they may participate in the PHMIS.
Section 1: Contractual Requirements and Role
Policy 1-1: PHMIS Contract Requirements

The Pinellas County Homeless Leadership Board (HLB), a governing body made up of elected officials, community leaders, and local non-profit organizations, created and implemented a ten year plan to end homeless 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 HLB will contract for and administer a contract for 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 comply with the stated requirements. Agencies will be granted access to the PHMIS software system after:
- The Participation Agreement (PA) has been signed with the HLB, and
- Agencies put into place the stated requirements in the PA.
- Users complete state required background screening; attend a User Training session; and the agency has completed a site visit.
  - All PHMIS users need to complete and pass a Level II background screening, prior to attending his or her first PHMIS training. PHMIS must ensure that each Member Agency conduct a criminal background check 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 check including fingerprinting prior to beginning work. PHMIS is a shared client information system, each potential user must have completed and passed a Level II background screening prior to attending their first PHMIS training.
  - By law, the HLB cannot ask for a copy of the results as proof of completion, therefore, each organization must attest to PHMIS compliance with background screening requirements.

Agencies agree to comply with the policies and procedures approved by the PHMIS Governance Committee.
**Policy 1-2: PHMIS Governance Committee**

A Governance Committee, convened by the HLB executive committee, representing stakeholders in the HMIS project, will advise all project activities. The committee schedule is set by the HLB Executive Committee (A current PHMIS Governance Committee Membership List may be obtained from the HLB Continuum of Care).

**Governance Procedures:**

The PHMIS Governance Committee guides this project, serves as the decision making body and provides advice and support to the HLB Continuum of Care.

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

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

- Determining the guiding principles that should underlie the implementation activities of the PHMIS, including participating organizations, consumer involvement and service programs;
- Selecting the minimal data elements to be collected by all programs participating in the PHMIS 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; and
- Assisting in the identification of funding streams for the HMIS

As a sub-committee of the HLB, the HMIS Governance Committee follows the protocol of the CoC.

Consensus of the group as a whole is considered by this committee to be the most useful and healthy means of making a decision. However, in the event that a consensus is not forthcoming the following voting regulations will be called upon:

**Meetings:** The HMIS Governance Committee shall meet every other month and as scheduled by the committee as a whole; Special meetings of the Members may be called by a majority of the Governance Committee.

**Quorum:** Those Members present at a regularly scheduled meeting will constitute a quorum. The act of a majority of the Members present shall be the act of the full Membership.

**Minutes of Meetings:** Minutes shall be kept of every meeting and shall include, at a minimum, the date, time and place of the meeting, the names of all who are in attendance, the topics discussed, the decisions reached and actions taken, any reports made, and any other information as may be deemed necessary by the Chair. The HLB will keep official copies of the minutes for a minimum of seven years or as is standard for HUD documentation.
Policy 1-3: PHMIS Management

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

Management Procedures:

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

HLB 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, Agency Administrators;
- Establishing a fee schedule for PHMIS licenses
- Annual and quarterly reporting to include but not limited to:
  - Annual Homeless Assessment Report
  - Homeless Point in Time County
  - Housing Inventory Chart
  - System Performance Measures
  - HUD NOFA Application; and
- Implementing software enhancements recommended by the PHMIS Governance Committee.
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 PHMIS principles, policies and procedures outlined in this document.

The Member Agency Procedures:

- 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 PHMIS principles, policies and procedures outlined in this document;
- Is responsible for all activity associated with agency staff access and use of the PHMIS data system;
- Is responsible for establishing and monitoring agency procedures that meet the criteria for access to the PHMIS 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;
- PHMIS bed inventory much be maintained in real-time: All Housing Providers are required to maintain a current bed inventory and notify PHMIS staff 5 business days in advance of a change to any beds at the facility; PHMIS will maintain the bed inventory within PHMIS;
- Agrees to allow access to the PHMIS System only to staff who have completed Security Awareness Training, HIPAA Training, Level II Background Screening, and been trained in the PHMIS system and who have a legitimate 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; and

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

- Assume responsibility for integrity and protection of client-level data entered into the PHMIS system;
- Ensure organizational adherence to the PHMIS Policies and Procedures;
- Communicate control and protection requirements to Agency Administrators and users;
- Authorize data access to agency staff and assign responsibility of the data;
- Monitor compliance and periodically review control decisions;
- Ensure that data is collected in a way that respects the dignity of the participants;
- Ensure that all data collected must be relevant to the purpose for which it is used that the data is entered accurately and on time;
- Provide prompt and timely communications of data, changes in license assignments, and user accounts and software to the PHMIS Systems Administrator; and
- Notify immediately the PHMIS Systems Administrator of any issue relating to system security or client confidentiality.
Policy 1-5: Member 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 Procedures:

The Agency Administrator will be responsible for duties including:

- Editing and updating agency information;
- Ensuring that access to the PHMIS is requested for authorized staff members only after they have:
  a. Received training;
  b. Satisfactorily demonstrated proficiency in use of the software; and
  c. Demonstrated understanding of the Policies and Procedures and agency policies referred to above
- Request the HMIS System Administrator to create passwords and grant licenses needed to enter the system;
- Ensuring that new staff persons are trained on the uses of the PHMIS software system, including review of the Policies and Procedures in this document and any agency policies which impact the security and integrity of client information;
- Notifying all users in their agency of interruptions in service;
- Serving as point-person in communicating with the PHMIS System Administrator;
- Facilitating timely reporting from the Agency she/he represents (unless the Agency has designated another person for this function); and
- Working cooperatively with the PHMIS technical staff and consultants
- Attending no less than three quarterly PHMIS Agency Administrator Meetings held by the HLB
  o If the Agency Administrator is unable to attend a meeting, they must send an alternate that is registered as Agency Administrator back up with PHMIS

The Agency Administrator is also responsible for the implementation of data security policy and standards, including:

- 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; and
- Detecting and responding to violations of the Policies and Procedures or agency procedures.

The HMIS System Administrator 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 PHMIS access suspended. Suspended licenses will not be re-activated until Agency Administrators review all materials pertaining to the specific suspension on the PHMIS Help Desk and pass a post-test evaluation.
Policy 1-6: User

All individuals at the Member Agency levels who require legitimate access to PHMIS 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 PHMIS System Administrator agrees to authorize use of the PHMIS only 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 PHMIS responsibilities.
- The Member Agency agrees to authorize use of the PHMIS 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.

Users are any persons who use the PHMIS for data processing services. 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 PHMIS 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**

PHMIS staff will coordinate ongoing training schedules for Agency Administrators and end Users. Training will occur on a regular basis. The schedule of trainings will be determined by the PHMIS staff.

**Training schedule:**

- Basic: Introduction to the PHMIS System (End User Training)
- Introduction to the PHMIS Project
- Review of applicable policies and procedures
- Connecting to the Internet
- Logging on to the PHMIS System
- Entering client information including demographic, placements and services, HUD data and case management

**Program Management Training:**

Overview of the PHMIS Project (Agency Administrator)

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

Each HMIS user is required to attend an annual refresher training; HIPAA; and Security Awareness Training. Failure to do so will result in an inactive license status until the training completed.
Policy 1-8: Amending Policies and Procedures

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

Amending Procedures:

- The HLB’s Data and System Performance Committee is responsible for review these policies and procedures annually. Suggested amendments from this committee will be forwarded to the PHMIS Governance Committee.
- Revisions to any HMIS related policy will be noted as revisions with an effective date.
- Policy and procedures are available upon request and the most recent revision will be provided. Previous editions will be maintained in an electronic database.
**Policy 1-9: Required Licensing Fees**

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

**Licensing Fee Procedures:**

The PHMIS shall evaluate licensing fees annually and discuss proposed changes with local funding entities. HLB HMIS Member Agencies, (unless they meet the qualifications to receive a subsidized license as outlined in Policy 1-10, price change will take effect during the next annual billing cycle.

Each HLB HMIS Member Agency is required to pay any associated fees listed below for licenses requested. The fees listed below are non-negotiable and are for a 12 month period ending one year from the date of payment receipt.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
<th>Fee</th>
</tr>
</thead>
<tbody>
<tr>
<td>New License</td>
<td>There is a one-time setup fee ($255), the annual license fee ($234) plus an admin rate ($25) to purchase a new license for HMIS. Includes advanced reporting license. Fees are per user.</td>
<td>$514/user*</td>
</tr>
<tr>
<td>Annual License Renewal</td>
<td>There is an annual license fee ($234). Includes advanced reporting license. Fees are per user.</td>
<td>$234/user*</td>
</tr>
<tr>
<td>Vendor Assisted Reports, System Changes, or Technical Assistance</td>
<td>There is a fee for support from the vendor to create any new reports. Fees are per report at the current vendor rate. Rates subject to change without notice. Will require upfront deposit to spec out report. Upfront deposit goes towards balance of report project.</td>
<td>$125/hour*</td>
</tr>
</tbody>
</table>

*Fee subject to change based on vendor pricing change.
**Policy 1-10: Subsidized Licensing Fees**

The HLB will provide subsidized licenses to PHMIS staff, HLB staff, and PHMIS Member Agencies who meet the following criteria:

- any program funded by the HUD Continuum of Care (CoC);
- whose organizational mission is to end homelessness; or
- any service providing assistance to homeless, Categories 1 – 4, as defined by HUD
  
  (Category 1 – Literally Homeless • Category 2 – Imminent Risk of Homeless • Category 3 – Homeless Under Other Federal Statutes • Category 4 – Fleeing/Attempting to Flee DV)

**Licensing Fee Objective:** Each HLB HMIS Member Agency Administrator will receive a subsidized license. Additionally, two subsidized licenses per program or service physical location will be granted, if needed. Additional subsidized licenses can be requested through the HLB Pinellas HMIS Help Desk (https://pinellashmis.zendesk.com/access/unauthenticated). Subsidized licenses will be granted upon a case by case basis from the HLB HMIS Governance Committee if there are subsidized licenses available.

For programs or services that need additional non-subsidized licenses, the Member Agency Administrator can make a request for additional non-subsidized licenses through the HLB Pinellas HMIS Help Desk (https://pinellashmis.zendesk.com/access/unauthenticated). An invoice will be generated for payment.

**Eligibility:** Basic need services that will be eligible for subsidized licenses in HLB HMIS are:

- **food** - soup kitchen, food pantry, and food banks
- **homeless diversion** - financial assistance providers who help current homeless individuals and families (defined by the HEARTH Act) exit to permanent housing (i.e. rapid re-housing or homeless prevention)
- **housing/shelter** - homeless emergency shelters, transitional housing, or permanent supportive housing listed in the housing inventory chart
- **clothing/drop-in center** - a one stop center where a variety of basic needs are given such as telephone use, mailing address, clothing, computer use, showers, laundry, etc., or small organization whose mission is to provide clothes to homeless children
- **homeless street outreach** - teams who contact and engage with homeless clients on the street or in local emergency/ transitional facilities
- **homeless child care slots** - dedicated programs that provide child care only to homeless children and families
- **travelers aid** – funds for transportation assistance for clients returning home

Generally, providers falling into the following categories would not be eligible for subsidized licenses but may be granted upon a case-by-case basis from the HLB HMIS Governance Committee if there are subsidized licenses available:

- Information and Referral
- Housing/Shelter provider not listed on the Housing Inventory Chart
- Non-Homeless diversion financial assistance
- Non-Homeless dedicated child care slots
- Tutor/Mentoring
- Legal Assistance
• Physical Health
• Behavioral Health
• Law Enforcement providing basic need social service not related to homeless outreach
  • All others not listed as eligible basic needs services
Section 2: Participation Requirements
Policy 2-1: Participation and Implementation Requirements

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

Participation Agreement Procedures:

Identification of Agency Administrator: All PHMIS 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 PHMIS users, the Member Agency must assign both an Agency Administrator and a back-up Agency Administrator to coordinate PHMIS activities for their organization.

The Agency Administrator responsibilities include:

- Editing and updating agency information;
- Ensuring that access to the Pinellas HMIS is requested for authorized staff members only after they have:
  - Received training;
  - Satisfactorily demonstrated proficiency in use of the software; and
  - Demonstrated understanding of the Policies and Procedures and agency policies referred to above;
- Granting technical access to the software system for persons authorized by the agency’s leadership by requesting the PHMIS System Administrator to create passwords and grant licenses needed to enter the system;
- Ensuring that PHMIS users have basic computer competency/skills to adequately use and navigate the PHMIS system;
- Ensuring that new staff persons are trained on the uses of the PHMIS software system, including review of the Policies and Procedures in this document and any agency policies which impact the security and integrity of client information;
- Notifying all users in their agency of interruptions in service;
- Serving as point-person in communicating with the PHMIS System Administrator;
- Facilitating timely reporting from the agency she/he represents (unless the agency has designated another person for this function); and
- Working cooperatively with the PHMIS staff.

Security Assessment: The CEO/President, Executive Director, or legal authorized officer of the Member Agency must complete the Agency Administrator Designation Form to assign the Agency Administrator position to a specific staff member within the Member Agency. Organizations new to the PMHIS system will need to attend an initial site visit with the Agency Executive Director or designee, Program Manager/Administrator (if applicable) and Agency Administrator with PHMIS staff member to assess and complete Agency Information Security Protocols. Agency IT staff may be asked to participate as necessary. Additionally, as the HLB will not risk the privacy and confidentiality of client information, PHMIS licenses will not be approved 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. It is the Member Agency’s responsibility to ensure that no one with these charges be allowed access to the PHMIS, as the HLB as the PHMIS lead agency is not allowed to view individual background screenings. Member Agency must complete an annual security review to ensure the implementation of the security requirements for the PHMIS.

The Agency Administrator is also responsible for the implementation of data security policy and standards, including:

- Follow the PHMIS Security and Privacy Plans (In Attachments)
- Administering agency-specified business and data protection controls;
- Administering and monitoring access control;
- Complete the Security Self-Certification each January
- Providing assistance in and/or coordinating the recovery of data, when necessary; and
- Detecting and responding to violations of the Policies and Procedures or agency procedures.

**Training:** Commitment of Agency Administrator and designated staff persons to attend training(s) prior to accessing the system online

**NOTE:** ALL Security Information paperwork needs to be complete and signed by Executive Director or designee in order for Member Agency Staff to attend training.

**Client Data:** Agencies must:

- Secure written permission from the client to enter the client’s data into the PHMIS.
- Secure a release of information from the client to share personal information with other agencies.
- 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 PHMIS staff immediately.

**HMIS Signage:** The HUD Data and Technical Standard requires as a baseline requirement that every Member Agency post a sign at each intake desk (or comparable location) that explains generally the reasons for collecting protected personal information (PPI). 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”.

**Initial Set-Up Site Visit:** Prior to signing any agreements for participation, a prospective PHMIS Member Agency must complete an initial site visit. This site visit will be completed at the prospective PHMIS Member Agency location. Participation in this site visit should be the PHMIS staff, the prospective PHMIS Member Agency Executive Director, 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 pertaining to Pinellas HMIS data entry, data quality or the reporting process. The goal for this site visit is to review the required data elements; PHMIS Policy and Procedures; define entry requirements; and set Member Agency expectations. The site visit also allows PHMIS staff to properly assess the prospective PHMIS Member Agency’s workflow, user needs, specific implementation issues, and any constraints or risks that will need
to be mitigated by the prospective PHMIS Member Agency prior to receiving access.

**Death, Disaster, Public Health Emergencies, or Public Safety:** Data within PHMIS 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 PHMIS staff will work closely with organizations, public officials, funders, and/or law enforcement to assist clients who are at risk. The PHMIS 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). The PHMIS staff will not print off, give an electronic copy of, or disclose any other personal information without a subpoena. However, in cases of death, PHMIS 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 HLB 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 PHMIS 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 HMIS 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, HMIS is an open or shared HMIS system. The default visibility settings for clients will be set to OPEN for all HLB 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, program visibility settings 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 PHMIS data
Policy 2-5: Client Consent for Electronic Data Sharing

All PHMIS 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:

Client Procedures from each Member Agency, including permission to enter data into the PHMIS system and release of information for sharing client data, must be on file at each agency.

Each Member Agency must publish the PHMIS 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. The PHMIS will maintain permanent documentation of all privacy notice amendments.

Member Agencies are obligated to provide reasonable accommodations 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 HIPAA policy will specify the purposes for which it collects data and will describe all uses and disclosures. **A Member Agency may use or disclose client data from the PHMIS only if the use or disclosure is allowed by the HUD HMIS Final Notice, and is described in this privacy notice. HIPAA regulations receive precedents over the HUD Final Notice PPI policies.**

PHMIS Policy requires written as well as oral consent as a fundamental component of the concept related to informed consent. Except for first party access to information and any required disclosures for oversight of compliance with PHMIS privacy and security standards, all uses and disclosures are permissive and not mandatory. Uses and disclosures not specified in the privacy notice can be made only with the consent of the individual or when required by law.

A 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 Final Notice - may reserve the ability to rely on the following reasons for denying an individual inspection or copying of the individual’s 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. A Member Agency that denies an individual’s request for access or correction must explain the reason for the denial to the individual and must include documentation of the request and the reason for the denial as part of the protected personal information about the individual.

Informed Consent Procedures:

Oral Explanation: All clients will be provided an oral explanation of the PHMIS. The Member Agency will provide an oral explanation of the PHMIS and the terms of consent. The agency is responsible for ensuring that this procedure takes place prior to every client interview. The Oral Explanation must contain the following information:

1. The PHMIS is a computer based information system that homeless services agencies across the community use to capture information about the persons they serve.

2. The CoC uses PHMIS to:
   - Understand their clients’ needs;
   - Help the programs plan to have appropriate resources for the people they serve; and
   - Inform public policy in an attempt to end homelessness

3. Only staff who work directly with clients or who have administrative responsibilities can look at, enter, or edit client records:
   - Clients have the right to not answer any question, **unless entry into a program requires it**
   - Client information is transferred in an encrypted format to the PHMIS database
   - Client has the right to know who has added to, deleted, or edited their PHMIS electronic client record

4. Benefits for clients:
   - Case manager tells client what services are offered on site or by referral through the assessment process
   - Case manager and client can use information to assist clients in obtaining resources that will help them find and keep permanent housing
**Informed Consent:** Is the process for gaining permission before entering data into PHMIS. An individual is to be asked to consent to their information being entered into PHMIS before creating a client entry. Informed consent must be based upon a clear appreciation and understanding of the facts, implications, and consequences of maintaining an individual’s information within PHMIS, including the sharing of this information with other organizations, to include but not limited to the HLB to give informed consent, the individual concerned must have adequate reasoning.

The original signed Client Informed Consent form should be kept by the PHMIS 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 the household may sign for any children or members of the household under the age of 18 on the same form. Once the written informed consent is obtained, it must be recorded in PHMIS and **is valid for 3 years**. After any PHMIS Informed Consent expires all clients still receiving services will need to sign another PHMIS Informed Consent Form and the data will need to be updated in PHMIS. Member Agencies are required to use the PHMIS Client Informed Consent form.

Written Client Consent to Share Data: Each Client whose record is being shared electronically with another Member Agency must agree via a written Release of Information (ROI) form 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:

**Release of Information (ROI):** Allows individuals access to their own PHMIS records and allows them control over to whom those records are released. PHMIS records should never be faxed and at this time are not permitted to be shared electronically.

The original signed Client Informed Consent form should be kept by the PHMIS Member Agency and protected from theft or loss. Release of information is specific to sharing data among providers in the Continuum of Care. Clients have the right to have their records open, partially open, or closed. The form must be completed by each member of the household receiving services who is over the age of 18 who does not sign the Informed Consent. The head of the household may sign for any children or members of the household under the age of 18 on the same form. Once a written release of information is obtained, it must be recorded in PHMIS and **is valid for 3 years**. After a PHMIS Release of Information expires, if the client is still receiving services when the ROI expires and the client chooses not to sign the Informed Consent, but still wants to control how their data is shared, they will need to sign another PHMIS Release of Information form and the data will need to be updated in PHMIS. Member Agencies are required to use the PHMIS Release of Information form provided.

The Member Agency understands that client identifiable data is inaccessible to unauthorized users. All clients who initially agree to participate in PHMIS have the right to rescind their permission for data sharing in PHMIS with the exception of those who have been entered into a financial assistance program. Clients who choose, and are permitted to, revoke their information sharing authorization must complete a new Release of Information (ROI).
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 PHMIS. 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 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 PHMIS 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.

- All PHMIS Member Agencies must obtain consent from all clients for whom they are entering or accessing client data into HMIS. Informed consent includes both an oral explanation and written client consent for each client.

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

At a minimum all rules, protocols, or procedures must address each of the following:

- 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 PHMIS 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 vendor
- Use of Anti-Spy ware, including the automated scanning of files as they are accessed by users on the system where the PHMIS 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 including 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 and hotspots should not be used by PHMIS users.

**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, or Satellite Downlink.
**Policy 2-9: Maintenance of Onsite (Agency) Computer Equipment**

The 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 PHMIS.

**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 PHMIS Project.

2. **Backup:** While the PHMIS 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 PHMIS. 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) of 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 that the guidelines associated with Data Disposal are properly followed.
Policy 2-10: Universal Data Elements

The PHMIS requires each HMIS Member Agency to enter client level data based on a set of predefined data standards.

Universal Data Element Procedures:

PHMIS 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 ServicePoint 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 from the HUD Exchange.

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

Policy 2-b: Program-Specific Data Elements

All Member Agency providers are encouraged to record all Program-Specific Data Elements (PSDE) for all clients entered into PHMIS even if not required for funding.

Program-Specific Data Element Procedures:

Optional PSDE are a valuable area of the client record and part of case management. Therefore, though 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 more effectively help the client.
**Policy 2-11: PHMIS Grievance**

The PHMIS Governance Committee holds the final authority for all decisions related to the governance of the PHMIS System. Decisions made or actions authorized by HLB regarding the PHMIS which do not satisfy an interested party, including those at the Continuum, agency or client levels, may be brought before the PHMIS Grievance Committee for a decision in accordance with the PHMIS Grievance Procedure. The Grievance Committee members shall 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 PHMIS, as these issues are most likely within a Member Agency. **It is only when the issue involves the actions of the PHMIS CoC operation that the PHMIS Grievance Procedure is to be used.** Additionally, the PHMIS 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 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 Administrator meet together with the appropriate PHMIS 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 PHMIS Governance Committee will convene the PHMIS Grievance Committee, giving them information concerning all actions taken to date:

1. The complaint is forwarded to the PHMIS Manager by the Member Agency’s Executive Director or designee.
2. The PHMIS Manager will staff the complaint with the PHMIS System’s Administrator and the HLB Executive Director or designee and prepare a written summary to be forwarded to the PHMIS Grievance Committee.
3. The PHMIS Grievance Committee will meet no later than ten (10) working days after being notified by the HLB regarding the formal complaint to hear the summary.
4. The PHMIS Grievance Committee will resolve the complaint within five (5) working days after this meeting.
5. Should the client want to appeal the PHMIS Grievance Committee’s decision, the PHMIS Governance 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 PHMIS 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 PHMIS staff concerning the PHMIS or any issue about which the PHMIS has
responsibility, they should first bring the matter to the attention of the PHMIS Manager 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 PHMIS party who has the ability
and authority to take corrective action. It is intended that discussion 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 PHMIS Governance Committee who will
   convene the Grievance Committee.
2. The Grievance Committee will meet no later than ten (10) working days 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 PHMIS Governance
   Committee, who will hear and resolve the complaint at its next regularly scheduled
   meeting. This decision is final.
Section 3: User, Location, Physical, and Data Access
**Policy 3-1: Access Levels for System Users**

User accounts will be created and deleted by the PHMIS Systems Administrator. There are different levels of access to the PHMIS. These levels are reflective of the access a user has to client level paper records. Access levels should be need-based. Any prospective PHMIS user should never have access to 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 member of its staff (including employees, volunteers, affiliates, contractors and associates) to sign (upon hire, and when modified) an end user agreement to acknowledges receipt of a copy of the 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 PA. Security measures exist within the PHMIS system which restricts agencies from viewing data not covered by this PA.

**Law Enforcement Access**

No active member of law enforcement or detention and corrections staff will be an authorized End User of Pinellas HMIS unless directly involved in Pinellas Safe Harbor.

**Procedure:** To protect current clients who may be accessing health and human service programs from harassment or harm, active members of law enforcement will not be granted access to Pinellas HMIS. Limited exceptions may be negotiated, and an agreement executed with the Director of HMIS & HLB concurrent to an agency's direct involvement in an active homeless outreach or jail diversion and/or prison release program. Any agreement with exceptions must include a statement that: PHMIS use is (1) limited to the purpose for which it was intended; and (2) is only for work with program-involved clients. PHMIS works with the Homeless Street Outreach Teams to ensure accurate data collection for unsheltered homeless clients. Homeless Street Outreach Teams consist of either or both an active member of law enforcement and a case worker. Either member may have access to PHMIS to assist in placing a homeless individual or family in a local shelter or housing unit. Former members of law enforcement who may volunteer or are employed at a homeless service provider post-law enforcement career may have access to PHMIS if it is imperative to their new responsibilities. PHMIS will consider and respond to requests by law enforcement for assistance with the following:

- 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;
- 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.

Pinellas HMIS will provide law enforcement information related to evidence and information gathering.
concerning a criminal matter via Court Order, such as a search warrant or subpoena. PHMIS will assist State Probation and Parole officials searching for individuals who are in violation of the probationary statutes.

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 Director.

**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 PHMIS, 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 PHMIS 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 PHMIS 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 user accounts will be the responsibility of the PHMIS Member Agency Administrator; the HLB will grant a unique user ID and password to all Authorized users.

**User Id and password procedures:**

- Each user will be required to enter a User ID with a Password in order to logon to the system
• User ID and Passwords are to be assigned to individuals.
• The 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 the PHMIS System Administrator and will be issued to the User by the Agency Administrator.
• The first time temporary password can be communicated via telephone or in person. Thereafter, passwords will be communicated in verbal form in person or via telephone only to the User. The Member Agency Administrator will reset a password if necessary. Passwords will not be sent via e-mail.
• Unsuccessful logon: If a User unsuccessfully attempts to logon three times, the User ID will be “locked out” on the next attempt and access permission will be revoked. The user will be unable to gain access until their password is reset in the manner stated above.

Policy 3-5: Right to Deny User and Member Agencies’ 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 PHMIS 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 PHMIS System Administrator.
5. PHMIS may restrict access prior to completion of formal investigation if deemed necessary by the PHMIS manager. If access is restricted, the PHMIS Manager will notify the Member Agency CEO and the chair of the 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 HLB, the PHMIS staff will permanently terminate the Member Agency from PHMIS. The PHMIS Member Agency’s 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 PHMIS Governance Committee.

9. Member Agencies seeking to be returned to full active PHMIS 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 HLB may be responsible for the cost to re-activate the license. This determination will be made by the PHMIS Governance Committee.
Policy 3-6: Data Access Control

Agency Administrators at Member Agencies and the PHMIS Manager reserve the right to monitor access to system software.

Data Access Control Procedures:

- Agency Administrators at Member Agencies and the HMIS Manager will regularly review user access privileges and deactivate users when users no longer require access.
  - The Pinellas HMIS staff will monitor all user licenses, license usage quarterly, and review and set licensing fees for the Pinellas HMIS system annually. It is the responsibility of the Pinellas HMIS Member Agencies to notify Pinellas HMIS when licenses are not being used by agency staff or when there is a turnover in agency staff that will impact the name on a license. Pinellas HMIS Member Agencies are to notify Pinellas HMIS within 5 business days of any licensing changes.
  - Quarterly license review will include:
    - PHMIS System Administrator will run a HMIS License Usage Report on a quarterly basis.
    - PHMIS Member Agency Administrators will be contacted when the system identifies a license that has not been used in the past 90-days.
    - PHMIS Member Agency Administrators will have 48 hours to confirm with PHMIS if this license is still needed by the agency. If PHMIS does not receive a response from a Member Agency within the 48 hour timeframe, the license will be revoked and put into the PHMIS License Pool.
- All requests for new or additional user licenses must be submitted in writing to the PHMIS Manager.
  - PHMIS will be adopting a new licensing fee schedule
- Agency Administrators at Member Agencies and the PHMIS Systems Administrator may implement discretionary access controls to limit access to PHMIS 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 the PHMIS Systems Administrator may audit unauthorized accesses and attempts to access PHMIS information.
- Access records shall be kept at least six months, and Agency Administrators and the PHMIS Systems Administrator may review the audit records for evidence of violations or system misuse.
Agency Administrators at Member Agencies and the PHMIS Manager reserve the right to monitor access to system software.

Data Access Control Procedures Continued:

Guidelines for data access control for the Member Agency:

- The federal regulations state that Physical Access to Systems with access to the PHMIS Data Computers that are used to collect and store PHMIS 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 through the use of an operating system such as Windows 2000, or Windows XP Pro, with individual profiles and system security policies enabled
- Each user should have a unique identification code.
- Each user’s identity should be authenticated through an acceptable verification process.
- Passwords shall be the responsibility of the user and shall not be shared with anyone.
- Users are able to select and change their own passwords, and should do so at least every ninety days.
- 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 3-7: Using PHMIS Data for Research

Agencies Member in the PHMIS 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.

PHMIS Data for Research Procedures:

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

- to provide or coordinate services to clients
- to 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
- for research purposes

PHMIS Release of Data for Research Conditions: The PHMIS Governance Committee will review and respond to requests for the use of PHMIS 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 PHMIS Governance Committee prior to publication, for publication approval by the HLB.
- Research will be shared with the appropriate agencies after publication.
- The HLB will be granted the rights to utilize all findings (results).
Section 4: Data Quality and Monitoring
Policy 4.1: PHMIS Data Quality Policy

PHMIS 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.

PHMIS Data Quality Procedures:

The HLB 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 PHMIS standards.

Data Quality Standard

- 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 document
- Blank entries in required data fields will not exceed the HUD error rate as per AHAR Participation Rules
- Data inconsistencies or missing data will not exceed the HUD error rate as per AHAR Participation Rules
- All PHMIS Member Agency client data should be entered no later than 24 hours after intake, assessment, or program or service entry or exit
  - In the event PHIMS 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
- A PHMIS Member Agency must maintain 95% or above in completeness of information entered into PHMIS
- 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 (See attachments)
  - The HLB will run and review Report 640, for all projects with entries and exits reports monthly
  - Agency Administrators will be trained on how to run and utilize Report 640 to correct data entry errors
  - If error rating for project rises above the acceptable target error percentage, the HLB will create a training course of action for the PHMIS users
  - If error rating for project continues to rise above the acceptable target error percentage, the HLB may implement corrective action, which would be monitored by the Data System and Performance Sub-Committee
- Bed inventory should be consistently maintained and managed to reflect true occupancy rates.
  - Inventories need to be sent to the PHMIS System Administrator within 5 business days of any changes.
  - PHMIS Staff will manage a centralized bed inventory
  - Agencies will be required to submit updated bed inventories to the PHMIS System Administrator quarterly, even if there have been no inventory updates
• Data entry must be complete within the timelines specified within the attached procedures
• All client data entered into PHMIS must match the PHMIS Member Agency client record/case file
• PHMIS Member Agency users should not assume client data or make changes to client data not reported by the client, unless the information has been officially verified.
  o Verification include but is not limited to: SSN confirmation; SSI confirmations; and/or Letters of employment or paystub information
• Any data errors identified by the PHMIS staff that has been submitted to the PHMIS Member Agency Administrators needs to be corrected within the time frame outlined by the PHMIS staff
• PHMIS Member Agency providers must conduct a search for existing clients in the system before adding a new client into the system
• All PHMIS Member Agency client data should adhere to HMIS font style guidelines
• All PATH SAMHSA-Funded clients who are no longer receiving PATH services or outreach should be exited in the system. If a client has gone sixty (60) days without service or contact, then they must be exited from the system
  o If a client is not enrolled for any reason, once PATH Status Determination information is recorded, and exit from the program should be added to the client record

Data Sharing and Data Quality:
For programs that share basic client-specific data, corrections and updates to client information will be made by the most current program. When duplicate information is found, the Agency will notify PHMIS immediately through contacting the PHMIS Help Desk.
Policy 4.2 Quality Monitoring

The PHMIS System Administrator will perform weekly, monthly, quarterly, and annual data integrity checks on the PHMIS data.

Data Quality Procedures:

Programs should run their PHMIS data completeness and timeliness reports on a weekly basis and the APR or equivalent annual report (for example, an ESG CAPER) monthly.

PHMIS Staff will:

- Run HUD Universal Data Elements, Data Incongruities Reports, and other data quality reports as determined by the CoC
  - Monthly, HLB will run and review Report 640, for all projects with Entry/Exits
  - If error rating for project rises above the acceptable target error percentage, the HLB will create a training course of action for the PHMIS users and Agency Administrator (See attachments)
  - If error rating for project continues to rise above the acceptable target error percentage, the HLB may implement corrective action, which would be monitored by the Data System and Performance Sub-Committee and reported to the PHMIS Governance Committee on a monthly basis until rectified
- Data completeness and data timeliness reports will be reviewed weekly/monthly by PHMIS staff to determine any patterns of data errors
- System Performance Measures will be competed monthly annually and reported to the HLB
- The HLB approved Dashboard Report will be submitted to the HLB monthly after approval from the Data and System Performance Committee
- Notify Agency Administrator of findings and timelines for correction
- The PHMIS staff will measure the bed utilization rates of homeless housing providers and publish it to the Internet in real-time
- PHMIS staff will conduct monthly reviews for duplicate data entries into the system and merge client records by hand. These merges will be applied to data entry error trends that are reported to the Agency Administrators
- Re-run reports for errant agencies/programs, as requested; following up with Agency Administrators, if necessary
- Notify Agency Executive Director if Agency Administrators are not responsive to required corrective actions
- Notify the CoC chair, PHMIS Manager, and the PHMIS Member Agency regarding any uncorrected data quality issues
- Responsible for reporting system errors and difficulties with HMIS working processes to the vendor. The PHMIS staff is at the will of the software provider to make all functionality changes to the system

Accountability for Data Quality:

- Any patterns of error at a Member Agency will be reported to the Agency Administrator through electronic mail
• When patterns of error have been discovered, users will be required to correct their data entry techniques, required to attend Pinellas HMIS training specific to the error trend, and will be monitored for compliance

• Programs with PHMIS PA’s will be considered to be out of compliance with their agreements 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 AHAR or funding reports are due at the same time)
  o Noncompliance to address data entry errors may result in a suspension of the Member Agency’s PHMIS user licenses.

• If data is not up to date, the HLB will take the following steps:
  o A formal letter of notification to the CoC Chair, Data and Data and System Performance Committee Chair, and Member Agency Executive Director
  o Inclusion of the status of non-compliance of the organization in HLB’s public reports
Section 5: Technical Support and System Availability
Policy 5-1: Technical Support

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

Technical Support Procedures:

The HMIS Manager, in conjunction with Agency Administrators and contracted third parties, will coordinate technical support services on a planned schedule with each Member Agency to:

- Assist Member Agencies on the use of Entry/Exit forms and other paperwork
- Conduct on-site 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 PHMIS 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 the PHMIS System Administrator have been developed:

- Service Request from Member Agency
  1. End user informs Member Agency’s Administrator of the problem.
  2. Member Agency’s Administrator attempts to resolve issue. If unable to resolve, agency staff is contact PHMIS System Administrator to request service.
  3. PHMIS System Administrator determines resources needed for service and if necessary, contacts vendor for support.
  4. PHMIS System Administrator will contact the Member Agency’s System Administrator to work out a mutually convenient service schedule and resolution to issue or concern.

- Chain of communication: (Problems should be resolved at the lowest possible level 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. Agency Staff
  3. PHMIS System Administrator
  4. PHMIS Manager
Policy 5-2: PHMIS Staff Availability

Consistent with the user’s reasonable service request requirements, HLB PHMIS staff is available for Technical Assistance, questions, and trouble-shooting between the hours of 8:30AM and 4:30 PM Monday through Friday.

Emergency Situations: Outside of normal business hours (8:30 AM to 4:30 PM Monday through Friday), contact the PHMIS Help Desk and leave a message. A PHMIS staff will respond by 8:30 a.m. the following business day.
Section 6: Training Information
**PHMIS Training Descriptions**

The PHMIS offers the following training opportunities for its users:

- **Agency Administrator Orientation**
- **Level 1 - Basic Data Entry**
  - A - Privacy and Security Training
  - B - Client/Shelter Basic Data Entry
  - HIPAA Certification*
  - Security Awareness*
- **Level 2 - Advanced Data Entry**
  - HMIS Case Management
- **Level 3 – Advanced Tools**
  - A – SkanPoint
  - B – ActivityPoint
  - C – Shelter Auxiliary Tool
  - D – Fund Manager
- **Level 4 - Basic Reporting**
- **Level 5 - Advanced Reporting**
  - A - Basics
  - B - Intermediate - Ad-hoc only
  - C - Advanced - Ad-hoc only

**PHMIS Agency Administrator Training:** Prerequisite: An executed HMIS Agency Administrator Designation form must be on file with PHMIS identifying the Agency Administrator in training. Prior to gaining PHMIS access as an Agency Administrator, the user will be required to complete training Levels 1, 2, and 4.

Every Agency Administrator must attend Agency Administrator Training. This training is specially designed to teach the Agency Administrator about how to communicate with the PHMIS staff and manage and monitor their HMIS data. Additionally, the class outlines the expectations required of Agency Administrators and how to request technical assistance from the PHMIS staff.

**Level 1: PHMIS Basic Data Entry:** Prerequisite: Basic computer competency or (if required) proof of completion of a basic computer competency course and copies of certifications from completed HIPAA and Security Trainings.

All PHMIS users must attend Level 1 training.

**A – PHMIS Privacy and Security Training:** This class will focus on clients’ rights and privacy and data security in HMIS.

**B – PHMIS Basic Data Entry:** This class focuses on the basic data entry requirements for entering all clients into the system. Training includes a discussion on the current HMIS forms (the HMIS user Agreement, HMIS Informed Consent, HMIS Style Guide, HMIS Privacy Notice, and the Housing Status Matrix). After training is administered all users must sign and adhere to the PHMIS end User Agreement then they will have access to the training site, and a “take home” test will be given where users will apply the knowledge they have learned in training. Users must complete the test within 5 business days of the training in order to be given access to the HMIS live site and keep
their license active. *This class is mandatory for all users.*

Level 2: PHMIS Advanced Data Entry: Prerequisite: Completed HMIS Level 1 training, passed the test, and were granted a license to the HMIS live site.

Level 2 is a continuation of Level 1 training for users who will be doing more advanced data entry and managing client case files in PHMIS. This class will discuss usage of the case management tools, VI-SPDAT, logging service outcomes, outstanding referrals, and managing duplicate clients. Users will have had access in the PHMIS live site, and post-training the features will be immediately available.

Level 2 is not required for all users.

Level 3: Advanced Tools: Prerequisite: Completed HMIS Level 1 training, passed the test, and were granted a license to the HMIS live site.

Level 3 focuses on modules in PHMIS that are not taught in the Levels 1 or 2. Level 3 is not required for all users.

**A - SkanPoint** - This class will teach usage of SkanPoint. Users will learn how to create ID cards for clients entered into PHMIS and how to use the ID card to rapidly scan clients into services, beds or in and out of a facility.

**B - ActivityPoint** - This class will teach usage of ActivityPoint. ActivityPoint is used as a flexible aid in establishing, scheduling, and managing day-to-day client events and activities, such as community educational sessions, volunteer sessions, field trips, and meetings. With this application, you can schedule activities from a single session, to sessions on a recurring basis. You can also manage and track participants and/or volunteers attending these events.

**C - Shelter Aux Tool** - This is a one on one tutorial for the large shelter providers who use this tool to track the on and off campus activity of the clients staying at the shelter. For information and training, contact the PHMIS Help Desk.

**D - Fund Manager** - This class will teach usage of administering a fund in Fund Manager. Funds Manager is the tool to see the real time use of dollars spent for financial assistance and rapid rehousing programs.

Level 4: PHMIS Basic Reporting: Prerequisite: Completed HMIS Level 1 training, passed the test, and were granted a license to the HMIS live site.

This Level 4 training is an overview of the reporting tab in the system and how to read data quality report cards. This class will focus on increasing knowledge of data quality basics and using the canned reports available in PHMIS. Reports overview will include: Client Served Report, Daily Unit Report, Service Transaction Report and Exit/Entry Report. Users are also introduced to the Data Quality and Timeliness Reports.

Level 4 is strongly encouraged for all users.
Level 5: PHMIS Advanced Reporting: **Prerequisite:**

- **Level 5 A:** Completed HMIS Level 1 training, passed the test, were granted a license to the HMIS live site, and completed Level 4 training.
- **Level 5 B:** Completed Level 5 A.
- **Level 5 C:** Completed Levels 5 A and B.

**A - ART Basics** - Required for all users with an ART Ad-hoc or Viewer license. This training will review the basics of the Advanced Reporting Tool (ART), how to access it, how to use the Gallery Reports, and how to run existing reports.

**B - ART Intermediate** - Required for all users with an ART Ad-hoc license who have completed Level 5A training. This training will introduce Agency Administrators to the basics of creating new reports in ART.

**C - ART Advanced** - Optional for all users with an ART Ad-hoc license who have completed Level 5A and B training. This training will build upon the ART Intermediate training and provide more complex concepts to improve new reports being developed in the system using the Advanced Reporting Tool (ART).

Level 5 is strongly encouraged for intermediate and advanced users.

*If your organization does not offer these type of trainings, the PHMIS staff will provide a link to the DCF HIPAA and Security Trainings.*
Section 7: Attachments
**Facts Sheet**

**FACT Sheet: Pinellas Homeless Management Information System (PHMIS)**

We will enter information you provide to us into a computer program called Homeless Management Information System (HMIS). We are doing this for several reasons:

- To find out what we need to end homelessness in Pinellas County;
- To provide better service;
- To receive federal funds.

**IMPORTANT POINTS ABOUT HOW YOUR INFORMATION WILL BE USED**

- We will use the PHMIS to keep a record of your contact with our agency.
- We will not share any information **without your written permission** through a signed client consent form that allows us to share client profile information with collaborating agencies. This means that you will not have to provide the same information at more than one intake.

**HOW WILL MY INFORMATION BE KEPT SECURE?**

- We have done several things to make sure that your information is kept safe and secure:
- The computer program we use has the highest security protection available;
- Any information that could identify you, like your name, SS# or birth-date, will be viewed only by people working to provide services to you, and will be removed before reports are issued to local, state, or national agencies;
- All employees agree to follow privacy rules before using the system.

**KNOW YOUR RIGHTS**

You have the following rights:

- To review your 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: PHMIS Governance Committee, in care of the HLB, 647 1st Ave. N., St. Petersburg, FL 33701, Attn: HMIS Manager.
Recommended System Tools for Best and Promising Practices for Quality HMIS

Using Case Management Tools – PHMIS Member Agency providers are encouraged to use the case management tools to track a client’s progress towards behavioral change and self-sufficiency.

**Summary:** PHMIS has several case management tools that will assist Member Agency providers in helping clients reach self-sufficiency. These tools include case notes, goals, action steps, tracking referral progress and the self-sufficiency outcomes matrix. Training for these tools are covered in PHMIS Level 2 training on case management.

Using Client Notes - PHMIS Member Agency providers are encouraged to use the shared case notes that will allow other Member Agencies to read about the client’s progress.

**Summary:** The sharing of case notes in PHMIS can be a great way of communicating with partners about the progress being made on shared clients. The case notes are meant to remind the client and service providers on the progress made and to be made by the client. Training for these tools are covered in HMIS Level 2 training on case management.

Using the VI-SPDAT - PHMIS Member Agency providers are encouraged to use the Vulnerability Index - Service Prioritization Decision Assistance Tool (VI-SPDAT) as an assessment tool for all clients that are entering and exiting in a program.

**Summary:** The VI-SPDAT is an assessment tool for each client in the PHMIS system and is a vital part of the Coordinated Entry System (CES). The VI-SPDAT is a pre-screening tool designed to quickly assess the health and social needs of homeless persons and match them with the most appropriate support and housing interventions within a community. It contains four assessment domains: History of Housing, Risks, Socialization and Daily Functions, and Wellness. Information about entering and using the VI-SPDAT in PHMIS is part of Level 2 Case Management training.

Creation of PHMIS Client Photo IDs - Member Agency providers are encouraged to create and disseminate PHMIS Client Photo ID Cards for all clients being entered into PHMIS.

**Summary:** The CoC has established the PHMIS Client Photo ID Cards as the identification for all homeless clients in the system. The cards may be issued at major continuum points of access such as day centers and one-stop centers or by other Member Agency providers when a service is rendered. PHMIS Client Photo ID Cards are covered in Level 3 training on SkanPoint.

Acceptance of PHMIS Client Photo IDs – PHMIS Member Agency providers are encouraged to accept the PHMIS Client Photo ID Cards for all clients for which they are providing services as proof of ID.

**Summary:** In order for the Continuum of Care and clients to see the benefit of ID cards, PHMIS Member Agency providers should be willing to generate, accept and ask for PHMIS Client Photo ID Cards from clients. This will require some education to the clients about the use of the ID cards and how it will help them access services better. PHMIS Client Photo ID Cards are covered in Level 3 training on SkanPoint.
PHMIS Client Photo IDs from Check-in – PHMIS Member Agency providers are encouraged to use the PHMIS Client Photo ID Cards for all clients for which they are providing services as proof of ID to rapidly check them into services and programs.

**Summary:** Using the barcode on the PHMIS Client Photo ID Cards, scan technology can help PHMIS Member Agency providers do business better. For low volume providers, scan technology can be used to access client records quicker. For high volume providers, scan technology can be used to check people into like services rapidly. PHMIS Client Photo ID Cards are covered in Level 3 training on SkanPoint.
SECURITY PLAN

Security Officers
The Homeless Leadership Board (HLB) has designated a Pinellas HMIS (PHMIS) 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 warehouse software, the methods of data exchange, and any PHMIS data or technical requirements issued by HUD. In the event that changes are required to the PHMIS Security Plan, the Security Officer will work with the PHMIS and the PHMIS Governance Committee for review, modification, and approval.
- Confirmation that the HLB adheres to the Security Plan.
- Response to any security questions, requests, or security breaches to the PHMIS and communication of security-related PHMIS information to Member Agencies.

Each Member Agency (MA)’s Agency Administrator must serve as the MA PHMIS 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 HLB PHMIS Security Officer, and security-related PHMIS information relayed from the PHMIS System Administrator to the Member Agency’s end users.
- Participate in security awareness training annually.

Annual Security Certification
The HLB and each MA must complete an annual security review to ensure the implementation of the security requirements for the PHMIS. This security review includes a completion of a security checklist, ensuring that each of the security standards is implemented in accordance with the PHMIS 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 HLB Security Officer no later than February 15 of each year.

Security awareness training and follow-up
All users must receive security training prior to being given access to the PHMIS. The HLB 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 HLB shall provide security training no less than once per year.
**Reporting security incidents**

The Homeless Leadership Board (HLB), PHMIS Lead Agency, has created the following chain of communication for reporting and responding to security incidents.

**Security Incidents**

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

**Reporting Threshold**

PHMIS 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 any and all security breaches that have the possibility to impact the PHMIS to the PHMIS Director.

**Reporting Process**

PHMIS end users will report security violations to their MA PHMIS Security Officer. The MA PHMIS Security Officer will report violations to the HLB PHMIS Security Officer. Any security breaches identified by Mediware Information Systems (ServicePoint) will be communicated to the HLB PHMIS Security Officer, PHMIS Director, and System Administrator. The PHMIS Director will review violations and recommend corrective and disciplinary actions to the PHMIS Governance Committee, as appropriate. Each Member Agency will maintain and follow procedures related to internal reporting of security incidents.

**Audit Controls**

Mediware Information Systems maintains an accessible audit trail within ServicePoint that allows the PHMIS System Administrator to monitor user activity and examine data access for specified end users. The PHMIS 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, smartphones, ipads, tablets, netbooks, mainframes and servers.

**User Authentication**

A MA must secure PHMIS 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 PHMIS 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 PHMIS 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 PHMIS system from malicious intrusion with a secure firewall. Each individual workstation does not need its own firewall, as long as there is a firewall between that workstation and any systems, including the Internet and other computer networks, located outside of the organization. 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 as long as the server has a firewall.

Physical Access to Systems with Access to PHMIS Data

A MA must staff computers stationed in public areas that are used to collect and store PHMIS 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 of time, staff should log off the data entry system and shut down the computer.
Hard Copy Security

A MA is to secure any paper or other hard copy containing personal identifiable information (PII) that is either generated by or for PHMIS, including, but not limited to reports, data entry forms, and signed consent forms. A MA must be present at all times any paper or other hard copy generated by or for PHMIS that contains PII is in a public area. When MA 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 PHMIS, regardless of whether the data has yet been entered into PHMIS, 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 PHMIS 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 PHMIS licenses held by the MA, and suspension of continued access to the PHMIS by the MA.
Disaster Recovery

PHMIS 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 PHMIS System Administrator will coordinate with Mediware Information Systems to ensure the PHMIS is functional and that data is restored. The HLB will communicate to MA’s when data becomes accessible following a disaster.

Contracts and other arrangements

The PHMIS Lead Agency shall retain copies of all contracts and agreements executed as part of the administration and management of the PHMIS 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 PHMIS Director, System Administrator, and Security Officer.
✓ Communicate security-related PHMIS information to the organization’s end users.
✓ Complete security training offered by the PHMIS Lead Agency.
✓ Additional duties specified in the PHMIS 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.

<table>
<thead>
<tr>
<th>Required policy</th>
<th>Meets Requirement (Yes/No)</th>
<th>If no, date by which compliance will be met</th>
</tr>
</thead>
</table>
| **User Authentication** | Does the agency abide by the PHMIS policies for unique user names and password? | All PHMIS 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 PHMIS? | 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 PHMIS
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-PHMIS computers if they are networked with PHMIS 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 PHMIS 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 PHMIS workstations in secure locations or are they manned at all times if they are in publicly accessible locations? (This includes non-PHMIS computers if they are networked with PHMIS 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 PHMIS are:  
In secure locations___Y______N  
Data Access:  
Users may access PHMIS 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 PHMIS workstations have current operating system and internet browser security? (This includes non-PHMIS computers if networked with PHMIS computers.)

<table>
<thead>
<tr>
<th>Operating System (OS) Version:</th>
</tr>
</thead>
<tbody>
<tr>
<td>_____________________________</td>
</tr>
<tr>
<td>All OS updates are installed</td>
</tr>
<tr>
<td>Y N</td>
</tr>
<tr>
<td>Most recent version of Internet browser(s) are installed</td>
</tr>
<tr>
<td>Y N</td>
</tr>
</tbody>
</table>

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 be in compliance within the timeframes stated above. This certification is incorporated into the PHMIS Participation Agreement. Any misrepresentation of the foregoing may result in termination of the Participation Agreement.

__________________________________________  ________________
PHMIS Security Contact Signature               Date

__________________________________________  ________________
Executing Officer Signature                    Date
Pinellas County HMIS • Homeless Leadership Board

PRIVACY PLAN

Each PHMIS MA must have a Privacy Statement that describes how and when the MA may use and disclose clients’ Protected 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,
5. 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
6. 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 PHMIS Lead Agency.
Stages of Implementation for New Member Agency

Prior to beginning Stage 1, a Member Agency needs to have:

- Completed security assessment, including all participation and data sharing agreements as well as client consent protocols;
- Identified an Agency Administrator; and
- Made proper connectivity arrangements. Because there is a great quantity of data transfer, the PHMIS requires that the Member agency have a Broadband Internet connection greater than 56K/90v. This includes DSL, Cable or Satellite Internet access. This Broadband Internet connection requirement will avoid lost staff time and staff frustration.

Stage 1. Planning

- Member Agency staff and PHMIS staff meet for the Security Assessment meeting.
- PHMIS staff and Agency Administrator will arrange a follow-up site visit to conduct operative tests on the program’s equipment, should this be needed.

Indicators to exit Stage 1: The Member Agency must complete all Stage 1 Activities before moving onto Stage 2 including signed PA (Participation Agreement) and Data Sharing Agreements returned to the PHMIS System Administrator.

Stage 2. Start-Up and Training

- To enter Stage 2, the Member Agency needs to have completed Stage 1.
- PHMIS System Administrator creates user IDs and temporary passwords for all users.
- Site users and the Agency Administrator receive training on uses of the PHMIS application. The Administrator training will include Program and Services Management.
- Trained agency staff work to enter client data into the system using the processes taught during training. These are different for HUD-funded agencies and non-HUD-funded agencies.

The PHMIS Stage 2 continues until data has been entered on 100% of clients served or for an entire month for all clients served within the Member Agency. This includes both basic client data, and program / service data required to support production of the HUD APR or other required reports.

Indicators to exit Stage 2: Interview protocols have been established including: Implementation of standard default interview protocols; use of interview protocols; and data entry including Entry and Exit transactions. Data have been entered on 100% of all new or current clients served within Member programs or for an entire month for all clients served within the Member Agency. Agency services have been defined in the HMIS and clients are being placed into them for an entire month.
Stage 3. Operational Status

To enter Stage 3 data entry must be completed for 100 % of clients served or for an entire month on all clients served.

Stage 3 of implementation:

- Member Agencies need to complete all Stage 2 Activities before moving onto the final Stage 3.
- Begins when staff utilizes the PHMIS System application to maintain client records, including service information.

Benefits of Stage 3 include the fact that client and service data becomes available for reporting purposes. Reports can be more easily generated such as: Standard reports including the HUD APR; demographics, including income sources, amounts and non-cash benefits; residential history patterns

Member Agencies will receive support from PHMIS staff to complete all stages. To ensure that all parties are comfortable with the process and progress for this stage, the Member Agency and PHMIS staff may meet again to assess if obstacles to progress exit.
Glossary

This glossary includes a list of terms that will be used throughout this document and by the HMIS staff.

**PHMIS**—Pinellas County Homeless Management Information System

**Agency Administrator (AA)**—A person designated by a Member Agency Executive Director/Chief Executive Officer who acts as a liaison and contact person to the Pinellas HMIS staff.

**AHCA**—Agency for Health Care Administration

**COC**—Continuum of Care

**DCF**—Department of Children & Families

**FDLE**—Florida Department of Law Enforcement

**F-SPDAT**—Family Service Prioritization Decision Assistance Tool - similar assessment to SPDAT designed for families.

**HHSCC**—Health and Human Services Coordinating Council

**HIPAA**—Health Insurance Portability and Accountability Act

**HLB**—HMIS Lead Agency, Pinellas Homeless Leadership Board, Inc.; Homeless Leadership Board, the Continuum of Care (CoC) Lead Agency

**HMIS**—Homeless Management Information System

**HUD**—Department of Housing and Urban Development

**Member Agency**—An agency who has signed all HMIS agreements and who is actively entering data into the system

**MOU**—Memorandum of Understanding

**PHMIS User**—Any user who has an active license to use ServicePoint; this can include Agency Administrators.

**Prospective Member Agency**—An agency who has inquired about joining HMIS

**ROI**—Release of Information

**ServicePoint**—software used to enter Pinellas HMIS data.
**SPDAT**—Service Prioritization Decision Assistance Tool.

**VI-SPDAT**—Vulnerability Index Service Prioritization Decision Assistance Tool—standardized assessment chosen by the Homeless Leadership Board and used to identify individual clients with the highest needs for housing.

**VI-FSPDAT**—Vulnerability Index Family Service Prioritization Decision Assistance Tool—similar assessment to VI-SPDAT designed for families.
## List of Acronyms and Abbreviations

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APR</td>
<td>Annual Progress Report</td>
</tr>
<tr>
<td>PHMIS</td>
<td>Pinellas Homeless Management Information System</td>
</tr>
<tr>
<td>CCS</td>
<td>HLB</td>
</tr>
<tr>
<td>CoC</td>
<td>Continuum of Care</td>
</tr>
<tr>
<td>DSL</td>
<td>Digital Subscriber Line (High-speed internet connection)</td>
</tr>
<tr>
<td>HIPAA</td>
<td>Health Insurance Portability and Accountability Act of 1996</td>
</tr>
<tr>
<td>HLB</td>
<td>Pinellas County Homeless Leadership Board</td>
</tr>
<tr>
<td>HUD</td>
<td>U.S. Department of Housing and Urban Development</td>
</tr>
<tr>
<td>PA</td>
<td>Participation Agreement</td>
</tr>
<tr>
<td>MA</td>
<td>Member Agency</td>
</tr>
<tr>
<td>PPI</td>
<td>Protected Personal Information</td>
</tr>
<tr>
<td>TA</td>
<td>Technical Assistance</td>
</tr>
</tbody>
</table>
## List of Revisions, Additions, and Deletions

<table>
<thead>
<tr>
<th>Original Issue</th>
<th>March 2005</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revision 8</td>
<td>October 2012</td>
</tr>
<tr>
<td>Revision 9</td>
<td>August 17, 2017</td>
</tr>
<tr>
<td>Revision 10</td>
<td>June 7, 2018</td>
</tr>
<tr>
<td>Revision 11</td>
<td>June 25, 2018</td>
</tr>
</tbody>
</table>
**Measure 1: Length of Time Persons Remain Homeless**

This measure the number of clients active in the report date range across ES, SH (Metric 1.1) and then ES, SH and TH (Metric 1.2) along with their average and median length of time homeless. This includes time homeless during the report date range as well as prior to the report start date, going back no further than October, 1, 2012.

**Metric 1.1: Change in the average and median length of time persons are homeless in ES and SH projects.**  
**Metric 1.2: Change in the average and median length of time persons are homeless in ES, SH, and TH projects.**

a. This measure is of the client’s entry, exit, and bed night dates strictly as entered in the HMIS system.

<table>
<thead>
<tr>
<th></th>
<th>Universe (Persons)</th>
<th>Average LOT Homeless (bed nights)</th>
<th>Median LOT Homeless (bed nights)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Submitted FY 2017</td>
<td>FY 2018</td>
<td>Submitted FY 2017</td>
</tr>
<tr>
<td>1.1 Persons in ES and SH</td>
<td>8143</td>
<td>7800</td>
<td>62</td>
</tr>
<tr>
<td>1.2 Persons in ES, SH, and TH</td>
<td>8640</td>
<td>8164</td>
<td>76</td>
</tr>
</tbody>
</table>

b. This measure is based on data element 3.17.

This measure includes data from each client’s Living Situation (Data Standards element 3.917) response as well as time spent in permanent housing projects between Project Start and Housing Move-In. This information is added to the client’s entry date, effectively extending the client’s entry date backward in time. This “adjusted entry date” is then used in the calculations just as if it were the client’s actual entry date.

The construction of this measure changed, per HUD’s specifications, between FY 2016 and FY 2017. HUD is aware that this may impact the change between these two years.
## FY2018  - Performance Measurement Module (Sys PM)

<table>
<thead>
<tr>
<th></th>
<th>Universe (Persons)</th>
<th>Average LOT Homeless (bed nights)</th>
<th>Median LOT Homeless (bed nights)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Submitted FY 2017</td>
<td>FY 2018</td>
<td>Submitted FY 2017</td>
</tr>
<tr>
<td>1.1 Persons in ES, SH, and PH</td>
<td>8348</td>
<td>7673</td>
<td>265</td>
</tr>
<tr>
<td>(prior to &quot;housing move in&quot;)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.2 Persons in ES, SH, TH, and PH (prior to &quot;housing move in&quot;)</td>
<td>8950</td>
<td>8011</td>
<td>279</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| 1.1 Persons in ES, SH, and PH  |8348                |7673                               |265                 |306     |41          |
| (prior to "housing move in")   |                    |                                  |                    |         |            |
| 1.2 Persons in ES, SH, TH, and PH (prior to "housing move in") |8950                |8011                               |279                 |314     |35          |
FY2018 - Performance Measurement Module (Sys PM)

Measure 2: The Extent to which Persons who Exit Homelessness to Permanent Housing Destinations Return to Homelessness

This measures clients who exited SO, ES, TH, SH or PH to a permanent housing destination in the date range two years prior to the report date range. Of those clients, the measure reports on how many of them returned to homelessness as indicated in the HMIS for up to two years after their initial exit.

After entering data, please review and confirm your entries and totals. Some HMIS reports may not list the project types in exactly the same order as they are displayed below.

<table>
<thead>
<tr>
<th>Exit was from</th>
<th>Total # of Persons who Exited to a Permanent Housing Destination (2 Years Prior)</th>
<th>Returns to Homelessness in Less than 6 Months</th>
<th>Returns to Homelessness from 6 to 12 Months</th>
<th>Returns to Homelessness from 13 to 24 Months</th>
<th>Number of Returns in 2 Years</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>FY 2018</td>
<td>% of Returns</td>
<td>FY 2018</td>
<td>% of Returns</td>
<td>FY 2018</td>
</tr>
<tr>
<td>Exit was from SO</td>
<td>0</td>
<td>0%</td>
<td>0</td>
<td>0%</td>
<td>0</td>
</tr>
<tr>
<td>Exit was from ES</td>
<td>1869</td>
<td>23%</td>
<td>136</td>
<td>7%</td>
<td>125</td>
</tr>
<tr>
<td>Exit was from TH</td>
<td>434</td>
<td>15%</td>
<td>19</td>
<td>4%</td>
<td>29</td>
</tr>
<tr>
<td>Exit was from SH</td>
<td>38</td>
<td>13%</td>
<td>1</td>
<td>3%</td>
<td>4</td>
</tr>
<tr>
<td>Exit was from PH</td>
<td>660</td>
<td>7%</td>
<td>32</td>
<td>5%</td>
<td>34</td>
</tr>
<tr>
<td>TOTAL Returns to Homelessness</td>
<td>3001</td>
<td>18%</td>
<td>188</td>
<td>6%</td>
<td>192</td>
</tr>
</tbody>
</table>

Measure 3: Number of Homeless Persons

Metric 3.1 – Change in PIT Counts
### FY2018 - Performance Measurement Module (Sys PM)

This measures the change in PIT counts of sheltered and unsheltered homeless person as reported on the PIT (not from HMIS).

<table>
<thead>
<tr>
<th></th>
<th>January 2017 PIT Count</th>
<th>January 2018 PIT Count</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Universe: Total PIT Count of sheltered and unsheltered persons</td>
<td>2831</td>
<td>2612</td>
<td>-219</td>
</tr>
<tr>
<td>Emergency Shelter Total</td>
<td>1294</td>
<td>1299</td>
<td>5</td>
</tr>
<tr>
<td>Safe Haven Total</td>
<td>36</td>
<td>40</td>
<td>4</td>
</tr>
<tr>
<td>Transitional Housing Total</td>
<td>349</td>
<td>308</td>
<td>-41</td>
</tr>
<tr>
<td>Total Sheltered Count</td>
<td>1679</td>
<td>1647</td>
<td>-32</td>
</tr>
<tr>
<td>Unsheltered Count</td>
<td>1152</td>
<td>965</td>
<td>-187</td>
</tr>
</tbody>
</table>

### Metric 3.2 – Change in Annual Counts

This measures the change in annual counts of sheltered homeless persons in HMIS.

<table>
<thead>
<tr>
<th></th>
<th>Submitted FY 2017</th>
<th>FY 2018</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Universe: Unduplicated Total sheltered homeless persons</td>
<td>9258</td>
<td>8718</td>
<td>-540</td>
</tr>
<tr>
<td>Emergency Shelter Total</td>
<td>8607</td>
<td>8180</td>
<td>-427</td>
</tr>
<tr>
<td>Safe Haven Total</td>
<td>155</td>
<td>221</td>
<td>66</td>
</tr>
<tr>
<td>Transitional Housing Total</td>
<td>1061</td>
<td>842</td>
<td>-219</td>
</tr>
</tbody>
</table>
FY2018 - Performance Measurement Module (Sys PM)

Measure 4: Employment and Income Growth for Homeless Persons in CoC Program-funded Projects

Metric 4.1 – Change in earned income for adult system stayers during the reporting period

<table>
<thead>
<tr>
<th></th>
<th>Submitted FY 2017</th>
<th>FY 2018</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Universe: Number of adults (system stayers)</td>
<td>208</td>
<td>220</td>
<td>12</td>
</tr>
<tr>
<td>Number of adults with increased earned income</td>
<td>12</td>
<td>17</td>
<td>5</td>
</tr>
<tr>
<td>Percentage of adults who increased earned income</td>
<td>6%</td>
<td>8%</td>
<td>2%</td>
</tr>
</tbody>
</table>

Metric 4.2 – Change in non-employment cash income for adult system stayers during the reporting period

<table>
<thead>
<tr>
<th></th>
<th>Submitted FY 2017</th>
<th>FY 2018</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Universe: Number of adults (system stayers)</td>
<td>208</td>
<td>220</td>
<td>12</td>
</tr>
<tr>
<td>Number of adults with increased non-employment cash income</td>
<td>42</td>
<td>74</td>
<td>32</td>
</tr>
<tr>
<td>Percentage of adults who increased non-employment cash income</td>
<td>20%</td>
<td>34%</td>
<td>14%</td>
</tr>
</tbody>
</table>

Metric 4.3 – Change in total income for adult system stayers during the reporting period

<table>
<thead>
<tr>
<th></th>
<th>Submitted FY 2017</th>
<th>FY 2018</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Universe: Number of adults (system stayers)</td>
<td>208</td>
<td>220</td>
<td>12</td>
</tr>
<tr>
<td>Number of adults with increased total income</td>
<td>50</td>
<td>83</td>
<td>33</td>
</tr>
<tr>
<td>Percentage of adults who increased total income</td>
<td>24%</td>
<td>38%</td>
<td>14%</td>
</tr>
</tbody>
</table>
## Metric 4.4 – Change in earned income for adult system leavers

<table>
<thead>
<tr>
<th></th>
<th>Submitted FY 2017</th>
<th>FY 2018</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Universe: Number of adults who exited (system leavers)</td>
<td>241</td>
<td>323</td>
<td>82</td>
</tr>
<tr>
<td>Number of adults who exited with increased earned income</td>
<td>22</td>
<td>40</td>
<td>18</td>
</tr>
<tr>
<td>Percentage of adults who increased earned income</td>
<td>9%</td>
<td>12%</td>
<td>3%</td>
</tr>
</tbody>
</table>

## Metric 4.5 – Change in non-employment cash income for adult system leavers

<table>
<thead>
<tr>
<th></th>
<th>Submitted FY 2017</th>
<th>FY 2018</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Universe: Number of adults who exited (system leavers)</td>
<td>241</td>
<td>323</td>
<td>82</td>
</tr>
<tr>
<td>Number of adults who exited with increased non-employment cash income</td>
<td>35</td>
<td>50</td>
<td>15</td>
</tr>
<tr>
<td>Percentage of adults who increased non-employment cash income</td>
<td>15%</td>
<td>15%</td>
<td>0%</td>
</tr>
</tbody>
</table>

## Metric 4.6 – Change in total income for adult system leavers

<table>
<thead>
<tr>
<th></th>
<th>Submitted FY 2017</th>
<th>FY 2018</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Universe: Number of adults who exited (system leavers)</td>
<td>241</td>
<td>323</td>
<td>82</td>
</tr>
<tr>
<td>Number of adults who exited with increased total income</td>
<td>54</td>
<td>79</td>
<td>25</td>
</tr>
<tr>
<td>Percentage of adults who increased total income</td>
<td>22%</td>
<td>24%</td>
<td>2%</td>
</tr>
</tbody>
</table>
FY2018 - Performance Measurement Module (Sys PM)

Measure 5: Number of persons who become homeless for the 1st time

Metric 5.1 – Change in the number of persons entering ES, SH, and TH projects with no prior enrollments in HMIS

<table>
<thead>
<tr>
<th>Submitted FY 2017</th>
<th>FY 2018</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>8622</td>
<td>8232</td>
<td>-390</td>
</tr>
</tbody>
</table>

Universe: Person with entries into ES, SH or TH during the reporting period.

Of persons above, count those who were in ES, SH, TH or any PH within 24 months prior to their entry during the reporting year.

Of persons above, count those who did not have entries in ES, SH, TH or PH in the previous 24 months. (i.e. Number of persons experiencing homelessness for the first time)

Metric 5.2 – Change in the number of persons entering ES, SH, TH, and PH projects with no prior enrollments in HMIS

<table>
<thead>
<tr>
<th>Submitted FY 2017</th>
<th>FY 2018</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>9200</td>
<td>8821</td>
<td>-379</td>
</tr>
</tbody>
</table>

Universe: Person with entries into ES, SH, TH or PH during the reporting period.

Of persons above, count those who were in ES, SH, TH or any PH within 24 months prior to their entry during the reporting year.

Of persons above, count those who did not have entries in ES, SH, TH or PH in the previous 24 months. (i.e. Number of persons experiencing homelessness for the first time.)
**FY2018 - Performance Measurement Module (Sys PM)**

Measure 6: Homeless Prevention and Housing Placement of Persons defined by category 3 of HUD’s Homeless Definition in CoC Program-funded Projects

This Measure is not applicable to CoCs in FY2018 (Oct 1, 2017 - Sept 30, 2018) reporting period.

Measure 7: Successful Placement from Street Outreach and Successful Placement in or Retention of Permanent Housing

Metric 7a.1 – Change in exits to permanent housing destinations

<table>
<thead>
<tr>
<th></th>
<th>Submitted FY 2017</th>
<th>FY 2018</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Universe: Persons who exit Street Outreach</td>
<td>610</td>
<td>501</td>
<td>-109</td>
</tr>
<tr>
<td>Of persons above, those who exited to temporary &amp; some institutional destinations</td>
<td>579</td>
<td>451</td>
<td>-128</td>
</tr>
<tr>
<td>Of the persons above, those who exited to permanent housing destinations</td>
<td>9</td>
<td>6</td>
<td>-3</td>
</tr>
<tr>
<td>% Successful exits</td>
<td>96%</td>
<td>91%</td>
<td>-5%</td>
</tr>
</tbody>
</table>

Metric 7b.1 – Change in exits to permanent housing destinations
## FY2018 - Performance Measurement Module (Sys PM)

<table>
<thead>
<tr>
<th>Universe: Persons in ES, SH, TH and PH-RRH who exited, plus persons in other PH projects who exited without moving into housing</th>
<th>Submitted FY 2017</th>
<th>FY 2018</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>7956</td>
<td>7478</td>
<td>-478</td>
</tr>
<tr>
<td>Of the persons above, those who exited to permanent housing destinations</td>
<td>2583</td>
<td>2488</td>
<td>-95</td>
</tr>
<tr>
<td>% Successful exits</td>
<td>32%</td>
<td>33%</td>
<td>1%</td>
</tr>
</tbody>
</table>

Metric 7b.2 – Change in exit to or retention of permanent housing

<table>
<thead>
<tr>
<th>Universe: Persons in all PH projects except PH-RRH</th>
<th>Submitted FY 2017</th>
<th>FY 2018</th>
<th>Difference</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1257</td>
<td>1096</td>
<td>-161</td>
</tr>
<tr>
<td>Of persons above, those who remained in applicable PH projects and those who exited to permanent housing destinations</td>
<td>1157</td>
<td>1023</td>
<td>-134</td>
</tr>
<tr>
<td>% Successful exits/retention</td>
<td>92%</td>
<td>93%</td>
<td>1%</td>
</tr>
</tbody>
</table>
This is a new tab for FY 2016 submissions only. Submission must be performed manually (data cannot be uploaded). Data coverage and quality will allow HUD to better interpret your Sys PM submissions.

Your bed coverage data has been imported from the HIC module. The remainder of the data quality points should be pulled from data quality reports made available by your vendor according to the specifications provided in the HMIS Standard Reporting Terminology Glossary. You may need to run multiple reports into order to get data for each combination of year and project type.

You may enter a note about any field if you wish to provide an explanation about your data quality results. This is not required.
## FY2018 - SysPM Data Quality

<table>
<thead>
<tr>
<th></th>
<th>All ES, SH</th>
<th>All TH</th>
<th>All PSH, OPH</th>
<th>All RRH</th>
<th>All Street Outreach</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Number of non-DV Beds on HIC</td>
<td>1514</td>
<td>1285</td>
<td>1452</td>
<td>1484</td>
<td>874</td>
</tr>
<tr>
<td>2. Number of HMIS Beds</td>
<td>1441</td>
<td>1261</td>
<td>1438</td>
<td>1443</td>
<td>793</td>
</tr>
<tr>
<td>3. HMIS Participation Rate from HIC ( % )</td>
<td>95.18</td>
<td>98.13</td>
<td>99.04</td>
<td>97.24</td>
<td>90.73</td>
</tr>
<tr>
<td>4. Unduplicated Persons Served (HMIS)</td>
<td>8403</td>
<td>8606</td>
<td>8651</td>
<td>8726</td>
<td>1229</td>
</tr>
<tr>
<td>5. Total Leavers (HMIS)</td>
<td>7350</td>
<td>7452</td>
<td>7617</td>
<td>7591</td>
<td>905</td>
</tr>
<tr>
<td>6. Destination of Don’t Know, Refused, or Missing (HMIS)</td>
<td>3053</td>
<td>3337</td>
<td>3636</td>
<td>3819</td>
<td>108</td>
</tr>
<tr>
<td>7. Destination Error Rate (%)</td>
<td>41.54</td>
<td>44.78</td>
<td>47.74</td>
<td>50.31</td>
<td>11.93</td>
</tr>
</tbody>
</table>