

Minutes

HMIS Advisory Committee Meeting

DATE 3/21/2025

TIME 11:30 AM

FACILITATED BY Carolyn Keyser, PEH

In attendance

Mustapha Berhan (YWCA), Nicholas Coulter (PCHO), Elizabeth Doll (Eagle Star Housing), Lisa Greer (YWCA), Danielle Huertas (RHA), Shawntrell Holley (RRH & PEH Board), Jennifer Keys (PEH), Carolyn Keyser (PEH), Heidi Markham (PEH), Becky Miglioratti (DHS), Shermond Reid (JPC), Norman Simmons (PEH), Janice Steimer (PEH), Ranessa Sutton (YWCA)

Agenda Items

(Please refer to the meeting slides for more details.)

1. **Updates:** Reviewed recent updates from HUD.
 - System Performance Measures (SPM) Reporting period began on 3/14/2025 and ends on 4/11/2025 at 8:00 PM EST. This report details the CoC's performance outcome measures for the year.
 - Point-In-Time/Housing Inventory Count (PIT/HIC) reporting is delayed; No date has been set.
 - The CoC has not received any information regarding data changes needed as a result of the Presidential Executive Orders.
2. **HMIS Policy and Procedures Manual Review and Update – Section 5:**

Recommendations/Comments:

 - Nick inquired about HMIS browser support for Apple products, as well as security product recommendations. HMIS seems to perform well on Macs and iPhones/iPads.
 - Multi-factor authentication (MFA) was discussed. HMIS does not currently support MFA, but they are working on building that into the system.
 - Carolyn will follow-up with WellSky on the above areas.
 - The group discussed the issue of lost or stolen equipment. This will be addressed in a later section of the Policies and Procedures.

- The need for regular Security Training was identified. In addition to having a security component in a user’s initial training, an annual security training will be put into place for all users.
- The group needs to come up with a good policy for mobile device usage.
- Many of the security and privacy issues need to be upheld and monitored by the agencies participating in HMIS. When we review the Agency Agreement, we should look at the language pertaining to this area.
- Carolyn shared a work-in-progress draft of section 5 of the Policies and Procedures. This draft is provided at the end of these minutes.

3. **Feedback to HUD on the Data Standards:**

The group feedback from last month’s question was reviewed.

Question: What data is most important to collect?

Responses:

- Reason for homelessness
- Length of time homeless
- Prior living situation
- Data that helps determine a client’s needs and eligibility – current homeless status, income, disabilities, medical, mental health, household size, personal safety, food needs
- Demographics: Age, identified gender, sexual orientation, race, nationality, primary language, socio-economic information

This meeting, the group was asked to type in their response to the question, “What HMIS data elements or questions need improvement?” The answers will be reviewed in the next meeting. The final feedback to HUD is due on May 31, 2025.

Action Items

- Read and review Section 6 of the HMIS Policy and Procedures Manual and prepare any suggestions for updates/additions.

Next meeting

April 18, 2025, at 11:30am via Zoom. (This meeting was canceled due to a majority of members being unable to attend.)

5. HMIS Software

PEH has contracted with WellSky Community Services (CS) to provide the HMIS software (web application) and to host the CoC's implementation.

Hardware, Connectivity and Computer Security Requirements

All CHO's are responsible for implementation, maintenance, security, and monitoring of all systems used to access HMIS with an expectation of maintaining/sustaining systems at adequate performance levels to efficiently perform job duties.

5 (a) Workstation Specification

The minimum desktop specifications for WellSky Community Services are:

- Desktop or laptop computer running a currently supported version of Microsoft Windows or Apple MacOS with all applicable updates and security patches installed. Microsoft Windows works best with WellSky Community Services.
- Monitor
- Internet connectivity -- highspeed connection recommended.
- Web Browser –Google Chrome or Microsoft Edge provide the best compatibility with WellSky Community Services. Browsers should be kept up to date with the most recent releases. Ideally, browser updates should be applied automatically. HMIS passwords should not be stored in the browser.

Security Hardware/Software

All devices accessing HMIS must be password protected. Passwords should never be shared or kept in visible locations. If they are written down, keep them in a secure location. The devices should automatically lock after no more than 15 minutes of inactivity. This can be configured on most computers by using password protected screensavers set to activate after 15 minutes (or less) of inactivity. All workstations accessing HMIS need to be protected by a firewall. If the workstations are part of an agency computer network, the firewall may be installed at a point between the network and the internet or other systems rather than at each workstation. Each workstation also needs to have anti-virus, anti-spyware, anti-malware programs in use and properly maintained with automatic installation of all application updates.

Agency Workstation Access Control

Access to the HMIS will be allowed only from computers specifically identified by the Participating Agency's Executive Director or authorized designee and HMIS Agency Administrator. Laptop computers will require an additional security statement indicating that they will not be used for unauthorized purposes from unauthorized locations.

Due to the confidentiality of information collected in HMIS, computers need to be located in areas where they are physically secure. Monitors/Displays should be positioned in a manner that prevents them from being easily seen by anyone except the user. Privacy screens should be used when necessary to ensure confidentiality of screen content. These same rules apply when working remotely, e.g. when working from home.
