West Virginia Statewide

Homeless Management Information System

Policies and Procedures Manual

2022

Wheeling/Weirton
Coalition to End Homelessness

West Virginia
Balance of State CoC

Huntington Cabell
Wayne CoC

Kanawha
Valley
Collective
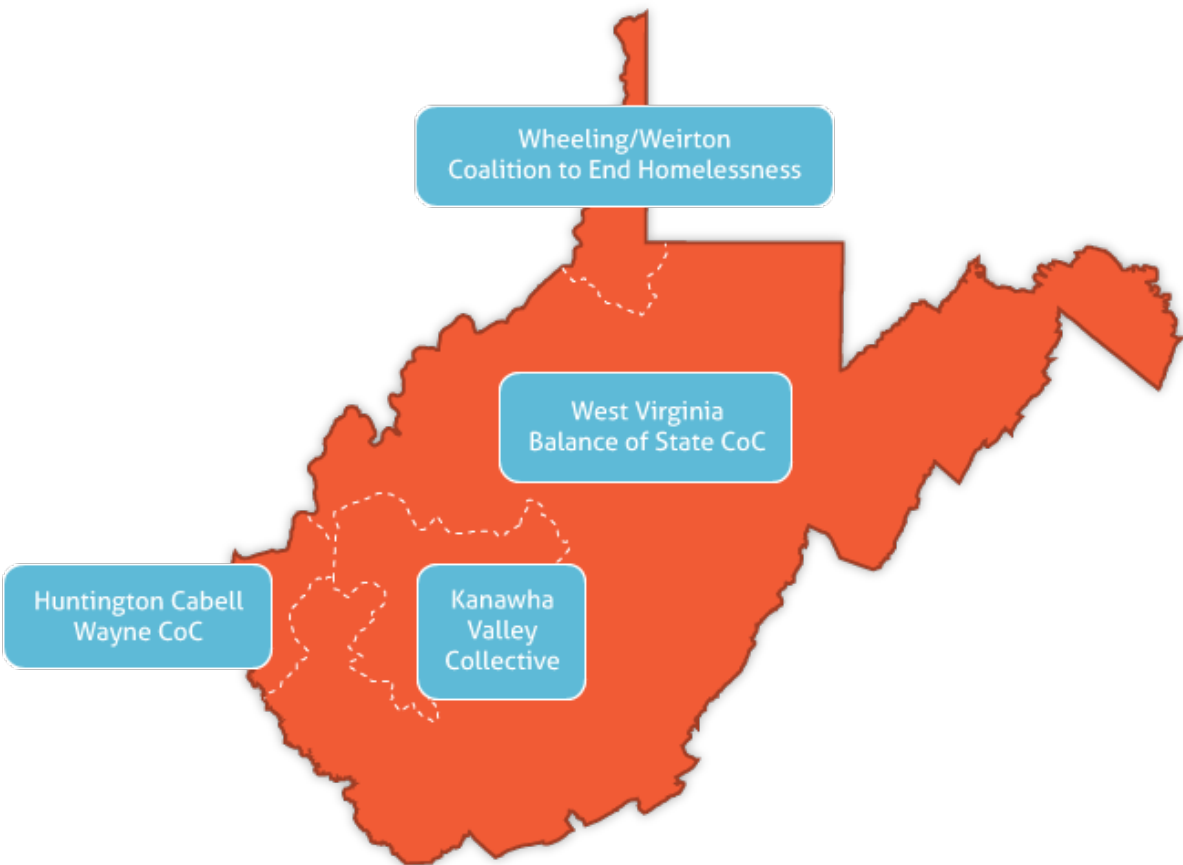
Contents

1. Introduction

The West Virginia Homeless Management Information System (HMIS) is a collaborative project of the four West Virginia Continuums of Care (CoC) – Balance of State (BoS), Kanawha Valley Collective (KVC), Cabell Huntington-Wayne (CHW), and Northern Panhandle Continuum (NPC) and participating Partner Agencies. HMIS is an internet- based database that is used by homeless service organizations across West Virginia to record and store client-level information about the numbers, characteristics, and needs of homeless persons and those at risk of homelessness. WellSky administers the central server and HMIS software (ServicePoint), and each CoC administers user and agency licensing, training, and compliance in their respective CoC.

HMIS enables service providers to measure the effectiveness of their interventions and facilitate longitudinal analysis of service needs and gaps at an agency, CoC, and Statewide level. CoCs were mandated by the United States Department of Housing and Urban Development (HUD) in the late 1990s to collect data regarding homeless populations as a condition of receiving federal funding, but they did not require any specific application. Use of HMIS is mandated by the U.S. Department of Housing and Urban Development (HUD) and by federal partners including the U.S. Department of Health and Human Services and the U.S. Department of Veterans Affairs, however, CoC's are encouraged to provide HMIS access to all homeless service providers within their service geography. Information that is gathered from consumers via interviews conducted by service providers is analyzed for an unduplicated count, aggregated (void of any identifying client level information) and made available to policy makers, service providers, advocates, and consumer representatives. Data aggregated from HMIS about the extent and nature of homelessness in the state of West Virginia is used to inform public policy decisions aimed at addressing and ending homelessness at local, state, and federal levels.

Guidance for the implementation of the West Virginia HMIS is administered by a broad-based Steering Committee which is representative of all West Virginia CoCs and is committed to understanding the gaps in services to consumers of the human service delivery system in an attempt to prevent and end homelessness. The make-up of the Statewide HMIS Steering Committee can be found on page 22.

The intent of this document is to provide the policies, procedures, guidelines, and standards that govern HMIS operations, as well as the responsibilities for System Administrators, Agency Administrators, End Users, and all others who access the West Virginia HMIS.

1.1. MISSION, VISION & VALUES

Mission:

The mission of the West Virginia Statewide HMIS is to facilitate and support the use of HMIS through training, data analysis, technical support, customer service, and system administration in an effort to end or prevent homelessness in West Virginia.

Vision:

The vision of the West Virginia Statewide HMIS is to operate a user-friendly data collection system that produces timely, accurate, and complete information for participants to use, ensuring the effective delivery of housing and services to end or prevent homelessness in West Virginia.

Values:

Accountability: A commitment to our clients and our communities that we will take responsibility for our actions and use data only in the pursuit of ending or preventing homelessness.

Partnership: We will collaborate with community partners in the gathering and sharing of knowledge.

Effectiveness: We will respond to issues through methodological, rational, and innovative thinking.

Integrity: We will operate with the best interest of the community and its members in mind.

Openness: We are committed to combating systemic bias by operating under an umbrella of informed consent, explaining data gathering methodology, and ensuring that access to services is kept open for all regardless of whether a client shares their personal information with any participating agency.

1.2. TERMINOLOGY

Many of the terms commonly used in homeless services, especially those in the WV Statewide HMIS Policies and Procedures, may be new to many readers. Understanding the common terms is crucial to understanding the roles, responsibilities, and functions of the WV HMIS.

Designated Agency HMIS Contact: This person is responsible for HMIS Administration at the participating agency level and is the primary contact between agencies and their CoC's System Administrator.

Annual Homeless Assessment Report (AHAR): The annual report to the U.S. Congress on the extent and nature of homelessness in America.

Annual Performance Report (APR): The HUD-required report used to track progress and accomplishments for CoC-funded projects.

Authentication: The process of identifying a user to grant access to a system or resource based on a username and password.

Client: An individual who has inquired about, is receiving, or has received services from a participating project about whom a participating HMIS project collects or maintains personally-identifiable information.

End User: A person that is responsible for entering client-level data for their agency. This person is also responsible for monitoring their data quality.

Executive Director: A person who serves as the top executive official of a participating agency. This is the person that is responsible for signing the Partnership Agreement.

HMIS: Homeless Management Information System: A local information technology system used to collect client-level data and data on the provision of housing and services to persons and families experiencing or at risk of experiencing homelessness.

HMIS Steering Committee: The group of CoC HMIS Staff who are responsible for approving and implementing the HMIS Policies and Procedures, and for working to make improvements to West Virginia HMIS.

HMIS License Fee: The annual fee paid by partner agencies to allow each HMIS User at their agency continued access to the database.

HMIS User Level: HMIS Users are assigned a specific user level that limits the data that user is able to access in the database.

HMIS Vendor: The West Virginia HMIS software vendor is WellSky. The HMIS vendor designs the software and provides ongoing support to HMIS System Administrators.

Housing Inventory Count (HIC): The inventory of beds available for persons experiencing homelessness, including HMIS, seasonal, and overflow beds.

Longitudinal System Analysis (LSA): A report required by HUD that is used for the AHAR. The LSA looks at data entered into HMIS, as well as data reported during the HIC and PIT.

Participating Agency: Any agency/project that enters client-level information into WV Statewide HMIS.

Point-in-Time (PIT): The annual count of sheltered and unsheltered persons and families experiencing homelessness on a single night in January.

Release of Information (ROI): A statement signed by the client authorizing or denying the participating agency/project to share their personal information, and information regarding their situation with other participating agencies.

Service Prioritization Decision Assistance Tool (SPDAT): A tool used to determine client acuity and level of need. SPDATs can be administered to singles, families, and transitional age youth.

ServicePoint: A software package administered and maintained by WellSky, which tracks data about persons in housing crisis to determine needs, services, and referrals and creates aggregate data for reporting and funding.

System Administrator: Staff in the CoC/HMIS Lead Agency who are responsible for overseeing HMIS users and use. System Administrators allow access, provide training, ensure compliance and data quality, and make policy recommendations to the WV Statewide HMIS Steering Committee.

Victim Service Provider (VSP): A non-profit agency with a primary mission to provide services to victims and survivors of domestic violence, dating violence, sexual assault, or stalking. VSPs are prohibited from viewing or entering data into HMIS. VSPs maintain data within a comparable database that is inaccessible to HMIS Users, Staff, and Administrators.

1.3. HMIS BENEFITS

Along with being HUD mandated and compliant, use of HMIS can provide numerous benefits for service providers, as well as persons experiencing homelessness.

Benefits for service providers:

- Provides online real-time information about client needs and the services available for persons experiencing homelessness.
- Enhances confidentiality by providing information in a secured system.
- Decreases duplicative client intakes and assessments, as well as any associated trauma that may come from the client reliving their experiences.
- Tracks client outcomes and provides a client service history.
- Generates aggregate data for local, state, and federal reporting requirements.
- Facilities the coordination of services within an individual CoC, as well as throughout the state.
- Provides access to a statewide database of service providers, allowing agency staff to easily select and track referrals across each CoC and throughout the state.
- Better defines and increases the ability to understand the extent of homelessness throughout West Virginia.
- Enhances the ability to focus staff and financial resources where services for persons experiencing homelessness are needed the most.
- Improves the capacity to evaluate the effectiveness of specific interventions, programs, and services provided.

Benefits for persons experiencing homelessness:

- Intake information and needs assessments are maintained historically, reducing the potential trauma and number of times a person experiencing homelessness must repeat their stories to multiple service providers.
- HMIS provides an opportunity for an intake and life history to be recorded one time. This demonstrates that service providers consider the time of the client as valuable and can lead to the restoration of a client's self-worth and identity.
- Multiple services can be easily coordinated and referrals can be streamlined and tracked over time.

2. Participating in HMIS

2.1. ROLES AND RESPONSIBILITIES OF THE STATEWIDE HMIS STEERING COMMITTEE:

The West Virginia Statewide HMIS Steering Committee is responsible for providing counsel and assistance to the staff members, governing bodies, and contributing providers within each of the

four continua of care on all matters regarding HMIS. The responsibilities of the steering committee include but are not limited to the following:

- Participate in decision-making and recommend policies and procedures regarding the statewide HMIS database and software system.
- Collaborate and support statewide HMIS activities.
- Disseminate information about the statewide HMIS database, the steering committee and its activities, policies, and procedures.
- Provide counsel and assistance to HMIS staff within each participating CoC.
- Identify, develop, and implement strategies for improving HMIS coverage and data quality throughout West Virginia.
- Provide support to individual CoCs in their efforts to identify and diminish potential barriers to the use and improvement of the statewide HMIS database.
- Safeguard client level data from unauthorized use or disclosure by developing and implementing policies, procedures, and practices centered around security, privacy, and confidentiality.
- Ensure the minimization of trauma and systemic bias by developing and implementing policies, procedures, and practices centered around client choice, consent, and accessibility.

2.2. STATEWIDE HMIS STEERING COMMITTEE MEMBERS

The West Virginia Statewide HMIS Steering Committee is a partnership of representatives from each of the participating continua of care. The committee is composed of two representatives from each continua of care and one representative from either the WV Community Advancement and Development Office, West Virginia Bureau for Behavioral Health & Health Facilities, or another WV state agency that administers homelessness related programs, for a total of nine members.

2.3. ROLES AND RESPONSIBILITIES OF HMIS USERS:

As mandated by HUD, each representative CoC sponsors the HMIS project within the Statewide Network. Operation of HMIS involves partnership between all four CoCs and each of their HMIS Lead Agencies and Partner Agencies.

System Administrators:

Each CoC appoints HMIS System Administration staff that provides end-user training and ensures that the Policies and Procedures are upheld by each Partner Agency within their respective CoC. System Administrators responsibilities include, but are not limited to, the following:

1) Provide representation on the Statewide HMIS Steering Committee.
2) Have full and complete access to all ServicePoint features and functions.
3) Generate reports for their respective CoC for local, state, and federal funding requirements.
4) Can make client records inactive, and delete needs and services created across organizational trees.
5) Provide Designated Agency HMIS Contacts and End Users with the most up-to-date information regarding changes with data collection requirements.

Designated Agency HMIS Contact:

Agency HMIS Contacts are designated by their individual agency, where appropriate. The Agency HMIS Contact acts as a point of contact between the agency's end users and the CoC's System Administrator(s). Agency HMIS Contact responsibilities include, but are not limited to, the following:

1) Ensure that the participating agency obtains a unique user license for each user at the agency in order to maintain security and integrity of client information.
2) Maintain a minimum standard of data quality by reviewing Data Quality Reports and ensuring all the HUD Universal Data Elements (UDE) and Program-Specific Data Elements (PSDE) are complete and accurate for every individual served by the agency and entered into HMIS.
3) Ensure agency staff receive required HMIS training, and review the West Virginia Statewide HMIS Policies and Procedures, the Agency Partner Agreement and any agency policies which impact the security and integrity of client information.
4) Ensure that access to HMIS is granted only to staff members that have received training, have completed the HMIS User Agreement, and are authorized to use HMIS.
5) Grant technical access to HMIS for persons authorized by System Administrators by resetting passwords and providing guidance to users outside of each CoC's required trainings.
6) Notify all users at their agency of interruptions in service.

7) Act as a single point of contact between users and HMIS staff at their respective HMIS Lead Agency.

8) Review and understand all correspondence sent by their respective HMIS Lead Agency.

9) Administer and monitor data security policies and standards including:

   a. User access control;

   b. Detecting and responding to violations of the statewide policies and procedures or agency procedures.

10) Identify the assessments and requirements for each program, and work with the System Administrator to properly set up each program in HMIS.

End Users:

HMIS End Users are those who have direct interaction with client-level data in the database. End Users have different levels of access to the system that are determined by their agency. End User responsibilities include, but are not limited to:

1) Take appropriate measures to prevent unauthorized data use or disclosure.

2) Report any security violations.

3) Know, understand, and comply with all relevant HMIS Policies and Procedures.

4) Input required data fields in a current and timely manner as outlined in the WV Statewide Data Quality Plan.

5) Ensure a minimum standard of data quality by accurately answering all the HUD Universal Data Elements and Program-Specific Data Elements for every individual entered into HMIS.

6) Inform clients about why their data is gathered, what the data will be used for, and who has access to the data.

7) Adhere to client requested-restrictions on data sharing.

8) Empower clients by informing them that they do not have to reveal their data in order to receive services.

9) Take responsibility for any actions undertaken with one's username and password.

10) Complete required training and all assignments associated with training as set forth by each user's CoC.

11) Review and understand all correspondence sent by their HMIS Lead Agency.

2.4. PARTNER AGENCY RESPONSIBILITIES

Partner Agency Authorization to Access HMIS-

The CoC HMIS Lead Agency will review all requests for access from new potential Partner Agencies. Requests for HMIS access will be granted to agencies that have a business interest in the HMIS. The HMIS Lead Agency will take into consideration the agency's intent to contribute data into the system or use HMIS data for the following: homeless service provision, referrals to non-homeless services used by persons experiencing homelessness or data analysis.

Participation Agreement Documents-

Partner Agencies must complete the following documents:

1) Partnership Agreements must be signed by each participating agency's Executive Director. The HMIS Lead Agency within each respective CoC will retain the original document. The participation agreement states the agency's commitment to adhere to the policies and procedures for effective use of HMIS. Partnership Agreements shall be updated annually.

2) End-User Account Requests shall be completed by the Agency Administrator (or other agency-designated individual) of each participating agency and submitted to the HMIS Lead Agency within their CoC. Account Request forms can be used to: add a user, delete a user, and change a user's name or access level.

3) End-User License Agreements, which list user policies and responsibilities, must be signed and submitted to the HMIS Lead Agency within their CoC by each authorized user. User Agreements shall be updated annually in order to maintain their license.

User License Eligibility-

Users must be paid staff or official volunteers of a Partner Agency. Individuals who are solely contracting with a Partner Agency are prohibited from receiving a user license. All users must be at least 18 years old.

User Access to the System-

- The Agency HMIS Contact will determine access for users at or below the Case Manager III access level and submit End-User Account requests to the HMIS Lead Agency within their CoC.
- The Executive Director, Agency HMIS Contact, and all users must complete the End-User License Agreement, and complete all necessary training requirements, as outlined by their CoC before access to the system is granted.

Tracking of Unauthorized Access-

Any suspicion of unauthorized activity should be reported to the HMIS staff within the user/agency's CoC. HMIS Staff will determine if there was unauthorized activity and take appropriate actions if such activity is confirmed.

Securing Client Informed Consent-

Agencies are required to ensure clients know what data are being collected about them and be given the opportunity to decide whether personal and program related information is shared in HMIS and with whom that data is shared as outlined in the Baseline Privacy Notice. Agencies are required to post the HMIS Consumer Notice in a location visible to clients when collecting client data and be able to provide a copy of the HMIS Baseline Privacy Notice upon client request. Agency staff are required to present the client with the most up-to-date Client Release of Information form made available from the Agency's respective CoC HMIS Lead Agency . The form allows the client to exercise their right to opt-out of data sharing in the cases where they have discretion.

Data Protocols:

Agencies participating in the HMIS must meet the minimum data entry requirements established under the most recently HMIS Data Standards. Agencies may collect information for data elements in addition to the minimally-required data elements established by HUD and its HMIS federal partners. Agencies must maintain consistency with data collection and entry within each program and communicate with the CoC System Administrator to ensure those data elements are added.

Agency Relationship with the HMIS Vendor-

Partner agencies are prohibited from directly contacting the HMIS Vendor to request custom database work. Any such request must be made through the HMIS Lead Agency.

2.5. USER COMFLICT OF INTEREST

It is every client's right to request inspection and possible correction of their data; however, in order to prevent users from editing their own files or files of immediate family members, all users will agree to a conflict of interest statement that is part of the User Agreement. Users shall disclose any potential conflict of interest to their Agency HMIS Contact (or other designated party). Users will be prohibited from making changes in their own file or the files of immediate family members. Any request for changes in their file should go to their Agency HMIS Contact (or other designated party). If a user is suspected of violating this agreement, the System Administrator will run an audit trail report to determine if there was an infraction.

2.6. PASSWORDS

- Creation: Passwords are automatically generated from the system when a user is created. The System Administrator will communicate the system-generated password to the user.
- Use: The user will be required to change the password the first time they log onto the system. The password must be at least 8 characters in length and contain at least 1 letter and 1 number. Passwords cannot be based on the user's name, common phrases, the user's place of work, or the programs they use. Passwords are the individual's responsibility and cannot be shared. Users are encouraged to not keep written copies of their passwords.
- Storage: If a user feels the need to write down their password, they must be inaccessible to other persons, stored securely, and not stored in a publicly accessible location. Passwords shall not be stored either on a computer's memory or saved on a website for easier access.
- Expiration: Passwords expire every 45 days. Users cannot use the same password consecutively. Passwords cannot be re-used until two password selections have expired.
- Unsuccessful logon: If a user unsuccessfully attempts to log-on three times, the User ID will be "locked out," and access permission will be automatically revoked rendering the user unable to gain access until their password is reset in the manner stated above.
- Password reset: Users that have been "locked out" can request that a system-generated password be sent to the email address associated with their user profile. Alternately, the user may request that a user with Agency Administrator permissions at their agency or their HMIS System Administrator manually reset their password. In either case, the user will be prompted to create a new permanent password before regaining access to HMIS.

2.7. USER TRAIINIING REQUUIREMENTS

- All new users are required to attend new user training offered by the HMIS Lead Agency within their CoC prior to receiving access to the system. If the HMIS Lead Agency determines that data entered by an End User does not meet minimum data quality standards, users will be required to repeat this training. Once a user begins the HMIS New User Training Series, the user has 30 days to complete the training series and all required assignments. If the user fails to complete all requirements within 30 days, the user will need to retake the training series.

- All users are required to attend annual security training to retain their user license.

- All users are required to attend additional HMIS trainings annually per the requirements set forth by their CoC. New user training will not count toward the general training requirements.

- In the event that a user does not use his or her license within a 90-day period, the account will be suspended, and the user will be required to take New User training again to get the license reinstated.

- All four CoCs have outlined their specific training requirements as an appendix to this document. Proceed to Appendix A to view the requirements for your CoC.

2.8. INPUTTING DATA

Agencies participating in HMIS shall meet the minimum data entry requirements established by HUD and its HMIS federal partners. Data should be entered into the system "live" with the client, or within three days (72 hours) of last contact with the client. Data for "mandated" programs shall follow the data entry guidelines established by the CoC's Standard Policies for each program type.

2.9. CLIENT CONSENT FORMS

All agencies are required to post the HMIS Privacy Notice wherever client data is gathered or stored. In addition, some agencies may require clients to sign an additional client consent form. The Privacy Notice informs clients of the electronic sharing of their personal information with other agencies that participate in HMIS when data sharing is appropriate for client service. It is the End User's responsibility to explain the Privacy Notice to the client in such a way that the client fully understands the implications and scope of data sharing. End Users are required to provide a copy of the Privacy Notice to the client should one be requested. Any written client consent must be

uploaded to the Release of Information (ROI) of the ClientPoint Workflow and dated two years from the date obtained.

2.10. HMIS USER LEVELS AND ACCESS

	Case Manager III	Agency Administrator	Executive Director	System Administrator I	System Administrator II	Read Only Access
Client Point						
Profile	X	X	X	X	X	X
Assessments	X	X	X	X	X	X
Case Notes	X	X	X	X	X	X
Case Plans	X	X	X	X	X	X
Service Records	X	X	X	X	X	X
Service Point						
Referrals	X	X	X	X	X	X
Services Provided	X	X	X	X	X	X
Resource Point	X	X	X	X	X	X
Shelter Point	X	X	X	X	X	X
Call Point	X	X	X	X	X	X
Administration						
Add/Edit Users		X	X	X	X	
Reset Passwords		X	X	X	X	
Add Provider				X	X	
Edit Provider		#	#			
Delete Provider		%	%			
Agency News	X	X	X	X	X	
System Wide News				X	X	
Provider Groups					X	
Pick list Data				X	X	
Licenses				X	X	
Assessment Admin				X	X	
Shadow Mode					X	
System Preferences					X	

X: Users have access to this section of ServicePoint.

%: Users can neither delete the provider to which they belong, nor any of their parent providers.

#: Users cannot edit their parent provider; they may only edit their provider or child providers.

Case Manager III:

Users may access all screens and modules except "Administration." A Case Manager III may access all screens within ClientPoint, including the medical screen. Users may access reports.

Agency Administrator:

Users may access all ServicePoint screens and modules. Agency Administrators may add/remove users and edit agency and program data for their agencies.

Executive Director:

Users have the same access rights as Agency Administrators, but rank above the Agency Administrator.

System Administrator I:

Users have the same access rights to client information as Agency Administrators, but for all agencies in the system. System Administrators also have full access to administrative functions.

System Administrator II:

There are no system restrictions on users. They have full HMIS access.

Read-Only Access:

Users can view, but not edit all screens within ClientPoint. User may access reports.

2.11. HMIS VENDOR REQUIREMENTS

The continua of care of West Virginia have opted to use ServicePoint as their HMIS software. ServicePoint is administered by WellSky. WellSky has provided industry-leading software systems to the human services industry for over 20 years.

Physical Security:

Access to areas containing HMIS equipment, data, and software shall be secured.

Firewall Protection:

The vendor shall secure the perimeter of its network using technology from firewall vendors. System Administrators employed by the vendor shall monitor firewall logs to determine unusual patterns and possible system vulnerabilities.

User Authentication:

Users may only access HMIS with a valid username and password combination that is encrypted via SSL (Secure Sockets Layer) for internet transmission to prevent theft. If a user enters an invalid password three consecutive times, they are automatically shut out of that HMIS session. For added security, the session key is automatically scrambled and re-established in the background at regular intervals.

Application Security:

HMIS users will be assigned a system access level that restricts their access to appropriate data.

Database Security:

Wherever possible, all database access is controlled at the operating system and database connection level for additional security. Access to production databases is limited to a minimal number of points; as with production servers, production databases do not share a master password database.

Technical Support:

The vendor shall assist the WV Statewide HMIS Steering Committee to resolve software problems, make necessary modifications for special programming, and will explain system functionality to the Statewide HMIS Steering Committee.

Technical Performance:

The vendor maintains the system, including data backup, data retrieval, and server functionality/operation. Upgrades to system software shall be continuously developed and implemented.

Hardware Disposal:

Data stored on broken equipment or equipment intended for disposal shall be destroyed using industry standard procedures.

2.12. MINIMUM TECHNICAL STANDARDS

Minimum Computer Requirements:

- A PC with a 2 Gigahertz or higher processor, 40GB hard drive, 512 MB RAM, and Microsoft Windows 8.1 or 10

- The most recent version of Google Chrome, Safari or Firefox. No additional plug-in is required. It is recommended that your browser have a 128 cipher / encryption strength installed. The browser's cache should be set to "Check for new version of the stored pages: Every visit to page."

- A broadband Internet connection or LAN connection. Dial-up modem connections are not sufficient.

- Virus protection updates

- Mobile devices used for HMIS data entry must use the Mozilla Firefox, Google Chrome or Apple Safari internet browsers. Apple Safari must be used on the latest version of iOS.

Additional Recommendations:

- Memory- Windows 8.1 or 10: 4Gig recommended (2 Gig minimum)

- Monitor- Screen Display: 1024x768 (XGA) or higher; 1280x768 strongly advised

- Processor- A Dual-Core processor is recommended

Password Protected Workstation:

- All workstations must be manually locked by a user if a licensed user leaves a workstation when ServicePoint is active. The system will automatically lock after fifteen (15) minutes of inactivity.

2.13.   HMIS LICENSE FEES AND OTHER ASSOCIATED COSTS

Each Continuum of Care within the WV Statewide HMIS Network will implement, maintain, and revise the fee structure, as well as the billing procedures, for any costs to Contributing Organizations associated with the use of HMIS within their CoC. Costs may include, but are not limited to, HMIS license fees, end user training, or custom reporting fees. Please refer to Appendix B of this document for CoC specific information on the HMIS fee structure.

Annual HMIS License Fees:

Agencies may purchase additional licenses at any time. Applicable CoC license fees are calculated on a per license basis and will be pro-rated to the first day of the month of purchase. As of the most recent version of this document, the annual cost of a new license and the on-going fees for each existing license allocated to the agency is determined by each CoC (Appendix B). Each CoC and the Vendor reserve the right to modify their fee structure.

In the event that a contributing agency's HMIS access is revoked by their CoC, the agency shall not attempt to gain access to HMIS in another CoC. All HMIS user licenses and associated costs are to be purchased/maintained from the CoC where the agency's main office is located. In the event of a contributing agency's service area crossing CoC lines, the CoC where the majority of services are provided will maintain the license.

2.14.   USE OF A COMPARABLE DATABASE BY VICTIM SERVICE PROVIDERS

Victim service providers, private nonprofit agencies whose primary mission is to provide services to victims of domestic violence, dating violence, sexual assault, or stalking, must not directly enter or provide data into HMIS if they are legally prohibited from participating in HMIS. Victim service providers that are recipients of funds requiring participation in HMIS, but are prohibited from entering data in HMIS, must use a comparable database to enter client information. A comparable database is a database that can be used to collect client-level data over time and generate unduplicated aggregated reports based on the client information entered into the database. The reports generated by a comparable database must be accurate and provide the same information as the reports generated by HMIS.

2.15.   HMIS OPERATING POLICIES VIOLATION

HMIS users and Partner Agencies must abide by all HMIS operational policies and procedures found in the HMIS Policies and Procedures manual, the User Agreement within their respective CoC, and the Partner Agency Agreement. Repercussion for any violation will be assessed in a tiered manner. Each user or Partner Agency violation will face successive consequences – the violations do not need to be of the same type in order to be considered second or third violations. User violations do not expire. No regard is given to the duration of time that occurs between successive violations of the HMIS operation policies and procedures as it relates to corrective action.

First Violation – the user and Partner Agency will be notified of the violation in writing by their respective CoC. The user's license will be suspended for 30 days, or until the Partner Agency notifies the CoC of action taken to remedy the violation. Each CoC throughout the statewide implementation will provide necessary training to the user and/or Partner Agency to ensure the violation does not continue. The respective CoC will then notify the Statewide HMIS Steering Committee of the violation during the next scheduled meeting following the violation.

Second Violation – the user and Partner Agency will be notified of the violation in writing by their respective CoC. The user's license will be suspended for 30 days. The user and/or Partner Agency must act to remedy the violation; however, this action will not shorten the length of the license suspension. If the violation has not been remedied by the end of the 30-day user license suspension, the suspension will continue until the Partner Agency notifies the CoC of the action taken to remedy the violation. The respective CoC will provide necessary training to the user and/or Partner Agency to ensure the violation does not continue. The respective CoC will then notify the Statewide HMIS Steering Committee of the violation during the next scheduled meeting following the violation.

Third Violation – the user and Partner Agency will be notified of the violation in writing by their respective CoC. The respective CoC will immediately notify the Statewide HMIS Steering Committee of the violation and determine if the user's license should be terminated. The user's license will be suspended until the Statewide HMIS Steering Committee decides. If the Statewide HMIS Steering Committee determines the user should retain their user license, the respective CoC will provide necessary training to the user and/or Partner Agency to ensure the violation does not continue. If users who retain their license after their third violation have an additional violation, that violation will be reviewed by the Statewide HMIS Steering Committee.

Any user or other fees paid by the Partner Agency will not be returned if a user's or Partner Agency's access to HMIS is revoked due to operating policies violation. The appropriate funder of the agency shall be notified of any operating policies violation that is not remedied in the allotted timeframe or if a Partner Agency's HMIS access is revoked.

Notifying the HMIS Lead Agency of a Violation:

It is the responsibility of the Designated Agency HMIS Contact or general User at Partner Agencies that do not have an HMIS Contact to notify the HMIS Lead Agency when they suspect that a User or Partner Agency has violated any HMIS operational agreement, policy or procedure. A complaint about a potential violation must include the User and Partner Agency name, and a description of the violation, including the date or timeframe of the suspected violation. Complaints should be sent in writing via postal mail or e-mail to the HMIS Lead Agency. The name of the person making the complaint will not be released from the HMIS Lead Agency if the individual wishes to remain anonymous.

Violations of Local, State or Federal Law:

Any Partner Agency or user violation of local, state or federal law will immediately be subject to the consequences listed under the Third Violation above.

Multiple Violations within a 12-Month Timeframe:

During a 12-month calendar year, if there are multiple users (three or more) with multiple violations (two or more) from one Partner Agency, the Partner Agency as a whole will be subject to the consequences listed under the Third Violation above.

3. Privacy and Security

The Department of Housing and Urban Development (HUD), with the HMIS Interim Rule, requires implementation of security standards. The importance of the integrity and security of HMIS cannot be overstated. Given this importance, HMIS must be administered and operated under high standards of data privacy and security. The Statewide HMIS Steering Committee, each Continuum of Care and Partner Agencies are jointly responsible for ensuring that HMIS data processing capabilities, including the collection, maintenance, use, disclosure, transmission and destruction of data, comply with the HMIS privacy, security and confidentiality policies and procedures. When a privacy or security standard conflicts with other Federal, state and local laws to which the Partner Agency must adhere, the Partner Agency must contact their respective CoC to collaboratively update the applicable policies for the partner agency to accurately reflect the additional protections.

3.1. PRIVACY AND SECURITY PLAN

The WV HMIS Steering Committee will set forth the administrative actions, policies, and procedures required to manage the selection, development, implementation, and maintenance of security measures to protect HMIS information detailed in the WV Statewide Privacy and Security Plan (Appendix C).

4. Data Requirements

4.1. MINIMUM DATA COLLECTION STANDARDS

Partner Agencies are responsible for asking all clients a minimum set of questions for use in aggregate analysis. These questions are included in custom assessments that are created by HMIS System Administrators. The required data elements depend on the program. The mandatory data elements in each assessment are displayed in red text and/or specific text indicating that the field is required.

The Designated Agency HMIS Contact or CoC System Administrator must identify the assessments and requirements for each program, and consult with the System Administrator(s) within their respective CoC to properly set up each program in HMIS.

Guidelines clearly articulating the minimum expectations for data entry for all programs entering data in HMIS will be sent to Designated Agency HMIS Contacts and posted on each CoC's webpage, if possible. HMIS Contacts must ensure that the minimum data elements and appropriate program-specific data elements are fulfilled by their agency.

4.2. PROVIDER NAMING CONVENTION

All providers within WV Statewide HMIS must be named so that they accurately reflect the type of service carried out by the corresponding Partner Agency program and the CoC where the agency is located in the following format: CoC- Agency- Project.

4.3. DATA QUALITY PLAN

Data quality is a term that refers to the reliability and validity of client-level data collected in the HMIS. It is measured by the extent to which the client data in the system reflects actual information in the real world. No data collection system has a quality rating of 100%. However, to meet the goals set forth by the WV statewide implementation when presenting accurate and consistent information on homelessness, it is critical that the HMIS have the best possible representation of reality as it relates to persons experiencing homelessness and the projects that serve them. Specifically, the goal is to record the most accurate, consistent and timely information in order to draw reasonable conclusions about the extent of homelessness and the impact on the homeless service system. To that end, each CoC will collectively assess the quality of our data by examining characteristics such as timeliness, completeness, and accuracy.

Data quality is vitally important to the success of the HMIS and the programs that use this database. HUD monitors the quality of the HMIS data through programs by the AHAR, LSA, and NOFA. If the quality of the data is poor, HUD may refuse to grant funding or trim future funding. Consequently, if this happens, these funding cuts could negatively affect program(s) throughout each CoC across the state of WV. Since it is imperative that the data is correct, HMIS Agency providers and the HMIS Staff from each CoC should be working diligently on adhering to the HUD data standards in order to ensure all reports are complete, consistent, accurate, and timely across the entire statewide implementation.

Partner Agencies are responsible for the overall quality, accuracy and completeness of data entered by their staff for their clients. HMIS staff within each CoC will regularly monitor data collection and hold participating agencies accountable for not entering required data or meeting the minimum data standards set forth in the WV Statewide Data Quality Plan (Appendix D).

4.4. DATA IMPORTS

While HMIS databases are required to have the capacity to accept data imports, each CoC reserves the right to not allow data imports into the West Virginia Statewide HMIS. Allowing data imports may impact data integrity and increase the likelihood of duplication of client files in the system.

4.5. HMIS DATA PROTECTION

Each HMIS Lead Agency within their respective CoC is responsible for maintaining the HMIS, including protecting the data contained in HMIS for the Statewide Network. In the case where the CoC is made aware through data contained in HMIS that Partner Agency program funds were used for an ineligible service, the CoC will notify the Partner Agency about the misuse of funds. If the Partner Agency fails to rectify the misuse of funds in a timely fashion, the CoC will notify the appropriate funding body.

5. FEDERAL HMIS REQUIREMENTS

5.1. HMIS REGULATIONS AND STANDARDS

The 2004 Data and Technical Standards Notice specifies describes the privacy and security standards for HMIS. The standards seek to protect the confidentiality of personal information while allowing for reasonable, responsible and limited uses and disclosures of data.

5.2. DATA DICTIONARY AND MANUAL

The HMIS Data Standards Manual is intended to serve as a reference and provide basic guidance on HMIS data elements for CoCs, HMIS Lead Agencies, HMIS System Administrators, and users. The companion document to the HMIS Data Manual is the HMIS Data Dictionary.

The HMIS Data Dictionary is designed for HMIS vendors, HMIS Lead Agencies, and HMIS system administrators to understand all of the data elements required in an HMIS, data collection and function of each required element and the specific use of each element by the appropriate federal partner. The HMIS Data Dictionary should be the source for HMIS software programming.

HMIS systems must be able to collect all of the data elements defined in the HMIS Data Dictionary, support system logic identified in this document, and ensure that data collection and the visibility of data elements is appropriate to the project type and federal funding source for any given project.

6. APPENDICES

Appendix A. CoC User Training Requirements
Appendix B. CoC HMIS Licensing Fees
Appendix C. WV Statewide HMIS Privacy and Security Plan
Appendix D. WV Statewide HMIS Data Quality Plan