Mid-Willamette Valley Homeless Alliance

HMIS LEAD

POLICIES & PROCEDURES

DRAFT

TABLE OF CONTENTS

1. Introduction and Purpose 2
2. Authority and Regulatory Framework 2
3. Definitions and Governing Terms 2
4. HMIS Governance 3
5. Participation Requirements 7
6. Victim Service Provider (VSP) Comparable Database Requirements 8
7. Privacy and Security plan 9
8. Data Collection and Quality 12
9. System Administration and Operations 13
10. Monitoring and Compliance 14
11. Reporting and Use of Data 17
12. Change Management 18
13. Training and Technical Assistance 20
14. Glossary of Terms 21

1. INTRODUCTION AND PURPOSE

The ORS 190 Entity, Mid-Willamette Valley Homeless Alliance (MWVHA), serves as the designated administrative entity for the U.S. Department of Housing and Urban Development (HUD) recognized Continuum of Care OR-504 (Marion and Polk Counties). OR-504 is the regional Continuum of Care membership body. MWVHA operates as the Collaborative Applicant and Homeless Management Information System (HMIS) Lead Agency for the region. Hereinafter, MWVHA is referred to as "the Alliance.

The purpose of this document is to promote transparency, provide clear guidance, and ensure compliance with HUD requirements under 24 CFR Part 578 and the HUD HMIS Data Standards. It serves as a single, comprehensive reference for the Alliance, consolidating multiple policies into one document that supports consistent HMIS governance, privacy, and operational practices.

This document establishes the authority and regulatory framework for HMIS operations, describing the governance structure and annual review/approval process. It defines participation and comparable database requirements, outlines privacy and security standards (including required signage), and specifies expectations for data elements, timeliness, and completeness. Additionally, it details system administration and operations such as vendor management, user account processes, and helpdesk support; sets forth monitoring, corrective action, and access revocation procedures; identifies required federal reports and local data use policies; explains how HUD data standards updates are implemented and communicated; and describes user training requirements, agency administrator roles, and technical assistance offerings.

2. AUTHORITY AND REGULATORY FRAMEWORK

- Responsibilities of the Continuum of Care: 24 CFR 578.7
- 2026 HMIS Data Standards Manual
- 2026 HMIS Data Dictionary
- 2004 HMIS Data and Technical Standards
- McKinney-Vento Act: 42 USC Chapter 119, Subchapter VI, Part B
- Hearth Act
- MWVHA Governance Charter
- ORS 190 Entity-MWVHA Bylaws
- HMIS Users Workgroup Governance Charter
- MWVHA Organizational Chart

3. DEFINITIONS AND GOVERNING TERMS

Agency Administrator: A staff member designated by each Participating Agency to serve as the primary liaison with the HMIS Lead. Responsibilities include managing user accounts, ensuring training compliance, and monitoring internal data quality and security to maintain a secure environment.

Client: Any individual or household receiving services, assistance, or referrals from a Participating or Partner Agency whose information is recorded in the HMIS for the purpose of service coordination, reporting, or performance measurement.

DRAFT

Comparable Database: A database maintained by a VSP that collects all HUD-required Universal Data Elements (UDEs) and Program-Specific Data Elements (PSDEs), generates required HUD reports, and complies with HUD privacy/security standards and VAWA confidentiality provisions.

Continuum of Care (CoC): The community-based planning body designated by HUD to organize and deliver housing and services to meet the needs of people experiencing homelessness. The CoC is responsible for coordinating funding, planning, and system-wide performance to prevent and end homelessness within its geographic area.

Homeless Management Information System (HMIS): Is a local information technology system used to collect client-level data and data on the provision of housing and services to individuals and families at risk of an experiencing homelessness.

HMIS Administrator: Individual(s) designated by the HMIS Lead to manage day-to-day HMIS operations. The HMIS Administrator is responsible for setting up user accounts, controlling access, configuring the system, monitoring data quality, troubleshooting issues, and providing technical support to participating agencies and end-users.

HMIS Lead: An organization designated by the Continuum of Care (CoC) to operate and manage the HMIS in compliance with HUD standards. The HMIS Lead is responsible for system administration, security, data quality oversight, user account management, and coordination of training and support for participating agencies.

HMIS User: An individual authorized by a Participating Agency to access and use the HMIS for legitimate business purposes. HMIS Users are responsible for entering, managing, and safeguarding client information in compliance with MWVHA's HMIS Policies & Procedures, Privacy and Security Plan, and all applicable data standards. Each User must complete required HMIS training and sign the MWVHA HMIS User Agreement prior to system access.

HMIS Users Workgroup: A CoC workgroup comprised of agency representatives and HMIS users, tasked with supporting data quality, reviewing policies, identifying barriers, and making recommendations to the HMIS Lead and CoC Board.

Participating Agency (Contributing HMIS Organization / CHO): Any organization or project required to enter data into HMIS as a condition of CoC, ESG, or state funding. This includes all CoC- and ESG-funded recipients/subrecipients, as well as other agencies that voluntarily participate.

System Administrator: The organization responsible for system configuration, license management, user account provisioning, coordination with the HMIS software vendor (WellSky), and ensuring the system's security, performance, and compliance with HUD data standards.

Victim Service Provider (VSP): An agency designated under the Violence Against Women Act (VAWA) that is prohibited from entering client-level data into HMIS. VSPs instead use a comparable database that meets HUD standards and submit de-identified aggregate data.

4. HMIS GOVERNANCE

HMIS ROLES AND DESIGNATION

HMIS Lead Agency/Administrator:
Mid-Willamette Valley Homeless Alliance

DRAFT

System Administrator:
Oregon Housing and Community Services (OHCS)

Software Vendor:
WellSky

AGENCY ADMINISTRATOR RESPONSIBILITIES

- Each Participating Agency must designate an HMIS Agency Administrator who serves as the primary point of contact with the HMIS Lead and serves on the HMIS Users Workgroup.
- Responsibilities include:
    - Ensuring agency staff complete required training before HMIS access is granted.
    - Monitoring compliance with HMIS policies, including privacy, security, and data quality requirements.
    - Serving as the first line of technical support within the agency before escalating issues to the HMIS Lead.
- Establish and follow internal agency protocols to escalate technical issues to the designated Agency Administrator before contacting the HMIS Lead.

Refer to Section 9: System Administration and Operations for the required account, access, and security standards that Agency Administrators must implement.

COC BOARD OF DIRECTORS, ORS 190 ENTITY RESPONSIBILITIES

The CoC Board oversees the work of the HMIS partners and retains final decision-making authority on key HMIS issues. It consults with the HMIS Users Workgroup on policy and operational decisions. The Board also designates representatives to serve on the Oregon Multi-CoC HMIS Governance Committee, ensuring regional alignment with state-level HMIS decisions.

In accordance with HUD requirements, the CoC Board must:

- Designate an HMIS Lead to operate and administer the HMIS.
- Develop and adopt an HMIS governance charter that, at a minimum, includes:
    - A requirement that the HMIS Lead enter into written HMIS Participation Agreements with each participating agency.
    - Any additional requirements issued by HUD or the CoC from time to time.
- Maintain documentation demonstrating compliance with HUD regulations and with the adopted governance charter.
- Review, revise, and approve policies and plans required by federal regulation, as well as any notices or requirements issued by HUD from time to time.

HMIS LEAD RESPONSIBILITIES

The Alliance serves as the HMIS Lead. It is responsible for the overall administration and operation of the HMIS in compliance with HUD regulations and CoC policies. Specific responsibilities include:

SYSTEM ADMINISTRATION AND OPERATIONS

- Provide operation, security, maintenance, system auditing, and technical support for HMIS hardware, software, and connectivity.

DRAFT

- Establish and manage user accounts, access levels, and passwords.
- Coordinate software updates, product upgrades, and technical troubleshooting.

POLICIES, PLANS, AND COMPLIANCE

- Develop, maintain, and annually update the HMIS Privacy Plan, Security Plan, and Data Quality Plan.
- Submit all HMIS plans and significant policy changes to the CoC Board for review and approval.
- Assess compliance with the CoC's HMIS Policies and Procedures Manual and enforce corrective actions when violations occur.
- Incorporate HUD Data Standards updates and communicate changes to participating agencies within required timelines.

Refer to Section 10: Monitoring and Compliance for more details on the requirements related to monitoring and compliance.

Refer to Section 12: Change Management for processes to implement HUD Data Standards updates and policy revisions.

AGENCY AGREEMENTS

- Maintain written HMIS Agency Agreements with all Contributing HMIS Organizations (CHOs).
- Maintain Comparable Database Agency Agreements with Victim Service Providers (VSPs).
- Impose sanctions for violations of agreements and enforce compliance, up to and including corrective action or funding impacts.

Refer to Section 10: Monitoring and Compliance for more details on the requirements related to monitoring and compliance.

TRAINING AND TECHNICAL ASSISTANCE

- Provide initial and ongoing training to HMIS users on system use, privacy, and security requirements.
- Coordinate and facilitate regular HMIS Users Workgroup.

Refer to Section 13: Training and Technical Assistance for more details on training requirements and enforcement.

DATA QUALITY AND MONITORING

- Conduct regular data quality checks, including monitoring timeliness, completeness, and accuracy of data entered by participating agencies.
- Provide technical assistance and guidance to agencies to correct identified data quality issues.
- Ensure consistent HMIS participation by all CoC and ESG recipients and subrecipients, in accordance with 24 CFR 578.7(b).

REPORTING AND DATA USE

- Generate and submit HUD-required reports required of the CoC, including but not limited to the Housing Inventory Count (HIC), Longitudinal Systems Analysis (LSA), Point-in-Time (PIT) Count and System Performance Measures (SPM) reports.
- Provide regular aggregate data reports to the CoC Board, and participating agencies to support planning, evaluation, and funding applications.
- Assist agencies with custom reports and queries for program evaluation and local planning needs.

DRAFT

GOVERNANCE AND COLLABORATION

- Collaborate with the HMIS Users Workgroup in policy development and implementation.
- Serve as the CoC's representative applicant to HUD for HMIS-related grant funds.
- Designate representatives to the Oregon Multi-CoC HMIS Governance Committee and participate in statewide HMIS governance activities to ensure alignment across regions.

HMIS USERS WORKGROUP RESPONSIBILITIES

The HMIS Users Workgroup supports CoC governance and the effective operation of the Homeless Management Information System (HMIS). The Workgroup is composed of Agency Administrators and serves as the primary forum for collaboration, feedback, and system improvement across participating agencies.

Responsibilities include:

- Identify Barriers – Reviewing and identifying barriers to the implementation of the CoC's Data Quality Plan and recommending strategies to address those barriers.
- Support Agencies – Ensuring participating agencies have the resources, training, and support needed to maintain timely, complete, and accurate data entry in HMIS.
- Review and Recommend HMIS Policies – Reviewing proposed HMIS policies and protocols and making recommendations to the HMIS Lead and the CoC Board for adoption and implementation.

ANNUAL REVIEW AND APPROVAL

The HMIS Users Workgroup is responsible for leading the annual review and recommending updates to HMIS policies and procedures, in coordination with the HMIS Lead.

Responsibilities include:

- Review the HMIS Privacy Plan, Security Plan, Data Quality Plan, and HMIS Policies and Procedures Manual at least once per year.
- Collaborate with the HMIS Lead to present updates or recommended revisions to the CoC Board of Directors for approval.
- Ensure documentation of CoC Board approval is maintained in official meeting records.
- Communicate approved updates, revisions, or new training requirements to all Agency Administrators through the HMIS Users Workgroup and email distribution.
- Ensure each participating agency disseminates updated guidance to its HMIS users and verifies completion of any required training.

SYSTEM ADMINISTRATOR RESPONSIBILITIES

Oregon Housing and Community Services (OHCS) serves as the statewide HMIS System Administrator for the State of Oregon. In this capacity, OHCS maintains authority over the HMIS software environment, vendor relationship, statewide configuration standards, and compliance with HUD HMIS Data Standards.

Within Continuum of Care OR-504 (Marion and Polk Counties), OHCS's authority as System Administrator operates in coordination with the designated CoC HMIS Lead Agency, the Mid-Willamette Valley Homeless Alliance ("the Alliance"). While the Alliance provides local HMIS

DRAFT

governance and oversight, OHCS retains final authority over system-level software management, statewide standards, and vendor administration.

OHCS responsibilities include, but are not limited to:

- Designate a single, centralized information system to serve as the official HMIS software for the geographic area.
- Maintain direct communication with the HMIS vendor to ensure consistent and reliable system support.
- Coordinate software updates, feature enhancements, and technical troubleshooting across participating agencies.
- Manage the vendor relationship, including contract administration, user licensing, and compliance with HUD HMIS requirements.
- Review and approve all changes to the HMIS software environment, including configuration settings, permissions, and data-sharing protocols.

Refer to Section 9: System Administration and Operations for the required account, access, and security standards that Agency Administrators must implement.

Refer to Section 12: Change Management for configuration, testing, and implementation of HUD Data Standards updates.

5. PARTICIPATION REQUIREMENTS

HMIS PARTICIPATION

In accordance with 24 CFR 578.7(b), all Continuum of Care (CoC) and Emergency Solutions Grant (ESG) recipients and subrecipients are required to participate in the Homeless Management Information System (HMIS) as a condition of funding.

Additionally, specific funding streams administered by the State of Oregon through the Oregon Housing and Community Services (OHCS) also require HMIS participation as a condition of funding. MWVHA executes these grant agreements with subgrantees on behalf of OHCS and ensures HMIS participation requirements are met.

Participating agencies must:

- Execute an HMIS Agency Agreement with the HMIS Lead Agency before entering data.
- Comply with all adopted HMIS policies and plans, including the Privacy Plan, Security Plan, and Data Quality Plan.
- Ensure staff are trained on HMIS policies and procedures, including privacy and security standards, before gaining access.

Failure to comply with HMIS participation requirements may result in corrective action, including loss of funding eligibility.

All participating agencies and users are required to maintain current HMIS Agency/User Agreements. User Agreements must be reviewed and updated at least annually, or more frequently as policies, systems, or data standards are revised.

Refer to Section 7: Privacy, Security, and Confidentiality for privacy and security requirements.

DRAFT

Refer to Section 10: Monitoring and Compliance for more details on the requirements related to monitoring and compliance.

ENFORCEMENT

Failure to comply with HMIS or comparable database participation requirements will result in corrective action or sanctions as outlined in Section 10 Monitoring and Compliance. Participating Agencies are expected to cooperate fully with monitoring activities and address identified issues within the timeframes established by the HMIS Lead and CoC Board.

6. VICTIM SERVICE PROVIDER (VSP) COMPARABLE DATABASE REQUIREMENTS

In accordance with the Violence Against Women Act (VAWA) and 24 CFR § 578.103(b), agencies designated as Victim Service Providers must maintain a HUD-compliant, comparable database rather than directly entering client-level data into HMIS.

COMPLIANCE WITH HUD STANDARDS

- Collect all HUD Universal Data Elements (UDEs) and Program-Specific Data Elements (PDEs).
- Maintain the capability to produce all HUD-required reports, including APR-equivalent, CAPER, and LSA-equivalent reports.

PRIVACY AND SECURITY

- Maintain a written Privacy Plan, Security Plan, and Data Quality Plan consistent with CoC policies and HUD HMIS Data Standards.
- Protect personally identifying information (PII) in compliance with VAWA confidentiality provisions and 24 CFR 578.103(b).

Refer to Section 7: Privacy, Security, and Confidentiality for privacy and security requirements.

DATA QUALITY AND REPORTING

Participating Agencies are responsible for maintaining high data quality standards and submitting accurate information in accordance with CoC, OHCS, and HUD requirements.

Responsibilities include:

- Submit de-identified aggregate data to the HMIS Lead according to the schedule and format outlined in the CoC Data Quality Plan and in compliance with OHCS and HUD reporting protocols.
- Provide aggregate reports from comparable databases in the required format and within the timelines established by OHCS and the CoC to ensure inclusion in system-wide reporting.
- Review and correct any data quality issues identified through CoC monitoring, HMIS Lead review, or HUD reporting processes within the designated correction period.
- Maintain ongoing data quality through regular internal reviews, adherence to data entry standards, and timely response to data quality notifications issued by the HMIS Lead.

AGENCY AGREEMENT

DRAFT

- Sign a Comparable Database Agency Agreement with the HMIS Lead, outlining roles, obligations, and compliance requirements.
- Participate in CoC-led data quality reviews and receive technical assistance as needed.

ENFORCEMENT

Failure to comply with VSP comparable database requirements will result in corrective action or sanctions as described in Section 10 Monitoring and Compliance. This includes potential impacts on funding eligibility and participation in CoC-led initiatives.

7. PRIVACY AND SECURITY PLAN

PRIVACY AND SECURITY PLAN

The Privacy and Security Plan establishes the safeguards, standards, and administrative procedures required to protect Personally Identifiable Information (PII) and ensure compliance with HUD's HMIS Data and Technical Standards, including the 2004 HMIS Data and Technical Standards governing allowable uses and disclosures.

This plan applies to the Alliance (as HMIS Lead), Oregon Housing and Community Services (as System Administrator), and all Participating Agencies that collect, enter, or access HMIS data.

This section consolidates all privacy, security, and confidentiality requirements into a comprehensive framework governing HMIS data protection, client rights, and user responsibilities. It defines the technical, physical, and administrative measures required to maintain system integrity, ensure secure data handling, and promote accountability across all HMIS partners.

All revisions to this Privacy and Security Plan apply to all HMIS data maintained within the system, regardless of the date of collection, unless otherwise prohibited by law.

ALLOWABLE USES AND DISCLOSURES

HMIS data may only be used or disclosed for purposes permitted under HUD's HMIS Data and Technical Standards, including:

- Provision and coordination of housing and services
- Administrative functions such as billing, monitoring, compliance, and system oversight
- Reporting to HUD and other authorized funders
- System performance measurement and evaluation
- Research activities approved in accordance with HUD standards
- As required by federal, state, or local law

Disclosures of client-level information without written client authorization may occur only when required by law, pursuant to a valid court order, or as otherwise expressly permitted under HUD standards.

All other disclosures require informed client consent.

DRAFT

PARTICIPATING AGENCY AND HMIS LEAD RESPONSIBILITIES

Participating Agencies and the HMIS Lead must:

- Comply with all applicable federal, state, and local privacy laws, including HIPAA and VAWA confidentiality provisions.
- Maintain and post a Privacy Notice at each intake and service location and make it available electronically upon request.
- Obtain and document client consent and Release of Information (ROI) before data sharing
- Ensure compliance with all security requirements described later in this section.
- Require all HMIS users to complete annual Privacy and Security training.
- Maintain system audit trails and activity logs for at least seven (7) years, consistent with Section 10: Documentation and Recordkeeping.
- Report any known or suspected security or privacy breach immediately, following Security Breach Protocol desc

PRIVACY NOTICE REQUIREMENTS

- Post a Privacy and Security Notice at each intake location, lobby, and other client service areas.
- Provide the Privacy Notice in writing upon request and publish it on the agency's website, if one exists.
- Inform clients at the time of enrollment how their data will be collected, used, stored, and shared.

CLIENT CONSENT AND RELEASE OF INFORMATION

- Obtain a signed HMIS ROI at each enrollment before sharing any client information with other agencies.
- Ensure each adult household member signs their own ROI; parents or guardians may consent for minors.
- Honor a client's right to refuse HMIS data entry or restrict data sharing without denying services (except where HUD mandates participation).
- Document and adhere to any client-imposed restrictions on data sharing.
- Record and maintain an active digital ROI in HMIS for each client to verify consent for data entry and authorized sharing.

CLIENT RIGHTS

Clients have the right to:

- Know what data is collected, how it is used, and with whom it is shared.
- Review their own HMIS record.
- Refuse to provide specific information.
- Request that their record or portions of their record be locked or made private.

SECURITY REQUIREMENTS

DRAFT

- Maintain secure internet access, current virus protection, an active firewall, an updated internet browser, and a password-protected screensaver that activates after five minutes of inactivity on all HMIS workstations.
- Assign each user a unique User ID and strong password; credential sharing is prohibited.
- Position computer screens to prevent unauthorized viewing of client data.
- Use HMIS IDs or de-identified information when transmitting data electronically; email and public Wi-Fi are not secure for PII.
- Secure any data printed, downloaded, or stored outside of HMIS.

Refer to Confidentiality Standards below for responsibilities related to printed materials and physical records.

CONFIDENTIALITY STANDARDS

- Prohibit disclosure of PII to entities outside the CoC's HMIS partners without client consent, except as permitted by law.
- Restrict access to areas where HMIS data is collected or stored to authorized personnel only.

The HMIS Lead shall not disclose client-level information to law enforcement agencies or representatives unless required by law, in response to a valid court order, or as part of a narrowly defined legal investigation authorized under federal statute (18 U.S.C. § 871 or § 879).

Routine or standing access to HMIS by law enforcement personnel, including for non-criminal, outreach, or public-safety purposes, is prohibited. Agencies affiliated with law enforcement may participate in HMIS only when the staff using HMIS are not engaged in enforcement, prosecution, or corrections activities, and only for legitimate service coordination consistent with HUD privacy standards.

Any disclosure to law enforcement must be documented, specifying the request, legal authority, data provided, and the approval of the HMIS Lead.

SECURITY BREACH PROTOCOL

Participating Agencies must immediately report any known or suspected breach of HMIS security or client confidentiality to the HMIS Lead.

- Identify and report breaches (including unauthorized access, loss or theft of information, or system compromise).
- Notify the HMIS Lead within 24 hours of discovery.
- Document incidents; the HMIS Lead will notify the CoC Board within five (5) business days and coordinate investigation and remediation with the vendor.
- Notify affected clients as required by federal and state laws.

Agencies that fail to report breaches promptly may be subject to corrective action, including suspension of HMIS access or funding impacts as described in Section 10: Monitoring and Compliance.

MONITORING AND ENFORCEMENT

DRAFT

- Conduct periodic data quality reviews, user audits, and site monitoring visits to assess compliance.
- Address non-compliance through corrective action, suspension of HMIS access, or funding impacts as determined by the CoC Board.

Refer to Section 10: Monitoring and Compliance for more details on the requirements related to monitoring and compliance.

8. DATA COLLECTION AND QUALITY

The Alliance and all HMIS Participating Agencies must collect, enter, and maintain client-level data in accordance with HUD HMIS Data Standards and CoC policies. Data collection and quality are crucial for ensuring accurate reporting, effective community planning, and compliance with federal and state regulations.

REQUIRED DATA ELEMENTS

- Collect and enter all HUD-required Universal Data Elements (UDEs) and applicable Program-Specific Data Elements (PDEs).
- Gather any additional data elements required by the CoC or state funding sources.
- Conduct direct client interviews whenever possible and document all collected data in client records.

TIMELINESS STANDARDS

- Enter client enrollment data into HMIS within three (3) business days of a program entry.
- Record client exit data within three (3) business days of program completion.
- Input service transactions and assessments within three (3) business days of service delivery.
- Maintain all active client records in current status and close them promptly when services end.

COMPLETENESS STANDARDS

- Complete all required data fields at the time of entry.
- Limit "Don't Know," "Refused," or "Data Not Collected" within the thresholds defined in the CoC Data Quality Plan.
- Review and correct records regularly to address missing or incomplete information.

ACCURACY STANDARDS

- Ensure that all data accurately reflects information provided by the client or supported by official documentation (e.g., identification, eligibility paperwork).
- Avoid making assumptions or altering client responses to fit program criteria.
- Verify and correct records routinely to maintain consistency across data elements.

DATA QUALITY MONITORING

- Conduct regular data quality reviews in alignment with the CoC's Data Quality Plan.
- Utilize automated reports, desk reviews, and on-site monitoring to assess data accuracy and completeness.
- Distribute data quality reports to agencies identifying errors, missing information, or timeliness issues, and require corrections within the specified timeframe.

CORRECTIVE ACTION

DRAFT

Agencies failing to meet data quality standards will be required to participate in targeted technical assistance. Ongoing monitoring, enforcement procedures, and potential sanctions for unresolved issues are detailed in Section 10: Monitoring and Compliance.

9. SYSTEM ADMINISTRATION AND OPERATIONS

The Alliance, as HMIS Lead, establishes and enforces the following system administration and operations standards. Participating Agencies and their designated Agency Administrators are responsible for implementing these requirements within their respective organizations.

USER ACCOUNT MANAGEMENT

- Assign each HMIS user a unique User ID and password.
- Ensure that each user account corresponds to a single individual; shared accounts are prohibited.
- Set user access levels based on job function and the principle of least privilege.
- Deactivate user accounts promptly when an individual separates from the agency, changes position, or no longer requires HMIS access for their job duties.

ACCESS AND AUTHENTICATION

- Require strong passwords (minimum of eight characters with upper/lower case, numbers, and special characters) and regular password changes for all user accounts.
- Implement two-factor authentication when supported by the HMIS vendor.
- Configure workstations to lock automatically after five minutes of inactivity and require re-authentication to resume access.
- Deactivate user accounts automatically after thirty (30) consecutive days of inactivity to maintain system security.

ADMINISTRATIVE ACCESS EXEMPTIONS

In limited circumstances, the HMIS Lead may authorize temporary or ongoing administrative permissions for designated staff or agencies when such access is necessary to fulfill programmatic, operational, or coordinated entry responsibilities.

Exceptions may be granted when the absence of access would significantly hinder the ability to perform duties essential to the Continuum of Care or a HUD-funded initiative.

These exceptions:

- Must be approved by the Alliance, in consultation with **OHCS** as appropriate;
- Must be documented in writing, specifying the staff, agency, scope, and purpose of access;
- Shall only be used for legitimate business purposes in compliance with all privacy, security, and data-sharing requirements; and
- Do not require separate CoC Board approval, as they fall within the administrative authority delegated to the HMIS Lead and System Administrator.

All exceptions will be reviewed during annual monitoring to ensure they remain justified, limited in scope, and compliant with HUD data standards and CoC policies.

DRAFT

LAW ENFORCEMENT ACCESS EXCEPTION

In limited cases, the HMIS lead may authorize access to programs affiliated with law-enforcement agencies provided those accessing HMIS are not directly involved in corrections/law enforcement, such as an outreach program. These cases will be evaluated with the HMIS Lead and OHCS, the System Administrator and contract holder for the HMIS database.

NOTE: No client-level information may be used for criminal investigation, prosecution or enforcement activities.

SYSTEM OPERATIONS AND MAINTENANCE

- The HMIS Lead will maintain vendor support agreements to ensure uptime, patching, and functionality.
- The system must undergo regular updates, including software upgrades, bug fixes, and feature enhancements as provided by the vendor.
- Routine system health checks and backups must be performed according to the vendor's specifications and CoC policies.
- Disaster recovery procedures must be documented and tested at least annually.

DATA SECURITY SAFEGUARDS

- Install and maintain current antivirus protection, firewall protection, and a supported internet browser on all devices accessing HMIS.
- Prohibit the use of public Wi-Fi and public workstations to access HMIS.
- Protect the physical security of any printed HMIS data by storing records in locked cabinets within locked offices.

TECHNICAL SUPPORT

- Provide or coordinate technical support for user access, account setup, password resets, error troubleshooting, and system performance issues.
- Establish and follow internal agency protocols to escalate technical issues to the designated Agency Administrator before contacting the HMIS Lead.

MONITORING AND COMPLIANCE

Monitoring and enforcement of system administration requirements will follow the processes described in Section 10: Monitoring and Compliance. Agencies found to be out of compliance with system administration or security requirements will be subject to corrective actions or sanctions as defined in that section.

10. MONITORING AND COMPLIANCE

The Alliance, as HMIS Lead, is responsible for monitoring compliance with HMIS policies, HUD HMIS Data Standards, and applicable federal and state regulations. The Alliance establishes and administers the monitoring framework described in this section. Participating Agencies and Victim Service

DRAFT

Providers (VSPs) are responsible for implementing HMIS requirements within their organizations and cooperating with monitoring activities.

The CoC Board retains final authority over enforcement actions and sanctions arising from monitoring findings.

MONITORING ACTIVITIES

Monitoring may be conducted on a scheduled, periodic, or risk-based basis as determined by the HMIS Lead.

Monitoring activities include, but are not limited to:

- Data Quality Reviews: Evaluation of timeliness, accuracy, and completeness of data entry, in accordance with benchmarks defined in the CoC's Data Quality Management Plan.
- Privacy and Security Compliance: Verification that users and agencies follow required privacy, confidentiality, and data-sharing standards.
- Agreement Verification: Confirmation that all Participation Agreements and User Agreements are current and properly executed.
- Training Compliance: Review of training records to confirm completion of required annual Privacy and Security training.
- Cybersecurity and Access Controls: Assessment of cybersecurity measures, including antivirus protection, firewalls, secure internet connections, and proper use of authentication protocols to prevent unauthorized access.
- Document and Data Storage Practices: Review of where and how agencies store HMIS-related documents and downloaded data to ensure secure storage (e.g., encrypted systems, locked file storage, and restricted access).
- Site Visits and Virtual Reviews: Evaluation of workstation placement, password protection, and adherence to system security and confidentiality requirements.

Refer to Section 7: Privacy, Security, and Confidentiality for privacy and security requirements.

ERROR THRESHOLDS

Error rates and quality standards are defined in the Data Quality Management Plan, which is incorporated by reference into this section. At minimum, HMIS participants must:

- Maintain a 95% completeness rate.
- Prevent "Client doesn't know/Client refused" responses from exceeding 10% for any field.
- Record client entry and exit data within three business days.
- Follow HUD's standards for Universal and Program-Specific Data Elements.

Errors may be categorized as minor, major, or systemic, depending on their frequency, scope, and severity, as determined by the HMIS Lead and the CoC Board in alignment with the Data Quality Management Plan.

Failure to meet data quality thresholds not only affects an individual agency. It can negatively impact the CoC's overall system performance, HUD reporting accuracy, and future funding opportunities. Persistent data quality issues can lead to a reduction in the CoC's competitive scoring in the HUD Continuum of Care Program Competition, which may result in reduced funding for the entire region.

DRAFT

All Participating Agencies share collective responsibility for maintaining data integrity to protect community resources and ensure accurate representation of homelessness within the CoC.

REPORTING AND FEEDBACK

Participating Agencies will receive monitoring reports identifying findings, concerns, and areas for improvement. Agencies must correct issues within the timeframe specified.

Agencies may request technical assistance to address compliance issues.

CORRECTIVE ACTION AND ENFORCEMENT

If monitoring identifies deficiencies, the HMIS Lead will initiate corrective action.

Corrective actions may include:

- Required technical assistance or additional training
- Increased monitoring frequency
- Temporary suspension of specific user accounts
- Development of a formal corrective action plan with defined timelines

If deficiencies are not resolved within the specified timeframe, the matter may be referred to the CoC Board for further action.

Sanctions for continued noncompliance may include:

- Suspension of HMIS access
- Withholding of reimbursement for CoC- or ESG-funded expenses
- Termination of grant agreements administered through the CoC
- Prohibition from applying for future funding opportunities administered by the CoC

Agencies that do not receive CoC, ESG, or state-administered funding are exempt from funding-related sanctions. However, access to HMIS may be limited or suspended to protect client confidentiality and system integrity.

DUE PROCESS

Prior to the imposition of sanctions, the HMIS Lead will provide written notice of noncompliance, proposed corrective action, and a response timeline.

Agencies may:

- Submit documentation demonstrating compliance
- Request technical assistance
- Provide a written response within the specified timeframe

Unresolved matters will be referred to the CoC Board for final determination.

COC BOARD OVERSIGHT

DRAFT

The CoC Board retains final decision-making authority on enforcement actions. The Board will review and approve monitoring frameworks, corrective action processes, and any proposed updates by the HMIS Lead or the HMIS Users Workgroup.

DOCUMENTATION AND RECORDKEEPING

The HMIS Lead will maintain complete documentation to demonstrate compliance with HUD requirements and CoC policies, including:

- Executed Participation Agreements and Comparable Database Agreements.
- User Agreements and annual training completion records.
- Data quality monitoring reports and agency corrective action plans.
- CoC Board minutes approving HMIS policies and updates.
- Documentation of any reported security incidents and their resolution.

All documentation will be retained for a minimum of seven (7) years, or longer if required by federal or state regulations, funding agreements, or ongoing audits. Records will be stored in a secure and accessible manner and made available for HUD monitoring or audit upon request.

Documentation may be reviewed by HUD, the State of Oregon, or authorized auditors upon request.

11. REPORTING AND USE OF DATA

The Alliance, as HMIS Lead, is responsible for generating and submitting all federally required HMIS reports and any additional reports required by the CoC Board of Directors. Participating Agencies are responsible for ensuring that client data entered in HMIS is accurate, complete, and timely to support required reporting.

REQUIRED FEDERAL REPORTS

The reports listed below will be produced in accordance with HUD guidance, system configuration requirements established by the System Administrator, and applicable reporting deadlines.

- Point-in-Time Count (PIT): Annual count of sheltered and unsheltered homeless persons.
- Housing Inventory Count (HIC): Annual inventory of housing resources dedicated to serving homeless persons.
- Longitudinal Systems Analysis (LSA): Annual system-level report submitted to HUD for national analysis.
- Annual Performance Reports (APR): Submitted for all CoC-funded projects, based on HMIS data.
- Consolidated Annual Performance and Evaluation Report (CAPER): Submitted for ESG-funded projects, based on HMIS data.
- Other reports as may be required by HUD, the State of Oregon, or other funders.

LOCAL DATA USE

The HMIS Lead may generate and distribute aggregate HMIS data to support system planning, performance evaluation, funding applications, and community reporting.

The HMIS Lead will:

- Provide aggregate HMIS data to the CoC Board for planning, performance measurement, and strategic decision-making.

DRAFT

- Prepare routine dashboards, data quality summaries, and system performance analyses for use by committees, workgroups, and partner agencies.
- Ensure that all distributed reports protect client confidentiality and do not include personally identifiable information (PII) unless authorized under applicable privacy standards.

The CoC Board retains final authority over the public release of aggregate HMIS data.

AGENCY REPORTING REQUIREMENTS

Participating Agencies are responsible for ensuring the accuracy, completeness, and timeliness of data entered into HMIS.

Agencies must:

- Review and certify agency-level HMIS data before the submission of any HUD-required report.
- Correct data errors identified through report validation processes within the timeframe specified by the HMIS Lead.
- Request project-level reports from the HMIS Lead as needed to support program evaluation, monitoring, and planning.
- Notify the HMIS Lead in writing within ten (10) business days of any changes to federal, state, local or private funding sources that may affect HMIS project configuration, reporting requirements or applicable data standards.

Refer to Section 8: Data Collection and Quality for standards that guide data validation and corrections

DATA SHARING AND PUBLICATION

The CoC Board and HMIS Lead share responsibility for deciding what data can be shared publicly and ensuring all published reports protect client confidentiality.

- Retain CoC Board authority to approve the public release of aggregate HMIS data.
- Review all reports intended for external publication to ensure compliance with privacy, security, and confidentiality standards.
- De-identify any data shared outside the CoC to ensure compliance with HUD and VAWA confidentiality requirements.

Refer to Section 7: Confidentiality Standards and Security Requirements for limits on sharing PII.

ENFORCEMENT

Failure to meet reporting requirements, including timely certification and correction of data errors, will be addressed through the corrective action and sanction processes outlined in Section 10: Monitoring and Compliance.

12. CHANGE MANAGEMENT

The Alliance, as HMIS Lead, is responsible for implementing and communicating changes to HUD Data Standards, HMIS system configuration, and related CoC policies within the OR-504 geographic area. Changes that affect the statewide HMIS platform or vendor configuration will be coordinated with Oregon Housing and Community Services (OHCS), as System Administrator.

DRAFT

The HMIS Lead will coordinate with the HMIS Users Workgroup, Participating Agencies, and the CoC Board of Directors to ensure timely compliance, effective communication, and continuous system improvement.

HUD DATA STANDARDS UPDATES

The HMIS Lead is responsible for reviewing, assessing, and implementing HUD-issued updates to the HMIS Data Standards and related guidance. Implementation of HUD-mandated changes will occur in accordance with HUD deadlines and statewide system configuration timelines established by the System Administrator.

- Review all HUD-issued updates to HMIS Data Standards, Notices, and Federal Partner reporting requirements upon release.
- Identify and summarize revisions to data collection elements, reporting formats, privacy and security requirements, or other HMIS-related policies.
- Assess the impact of required changes on system configuration, reporting, training, and agency workflows.

Refer to Section 4: System Administrator Responsibilities for vendor oversight responsibilities related to system configuration.

Refer to Section 7: Privacy, Security, and Confidentiality for privacy and security requirements.

POLICY AND PROCEDURE REVISIONS

The HMIS Lead, in collaboration with the HMIS Users Workgroup and CoC Board, is responsible for maintaining current compliant HMIS policies and procedures. Final authority for policy revisions rests with the CoC Board of Directors.

- Update the HMIS Policies and Procedures Manual to reflect new HUD requirements and operational changes.
- Review draft revisions through the HMIS Users Workgroup prior to submission to the CoC Board for final approval.
- Distribute approved policy updates to all Participating Agencies within thirty (30) days of CoC Board approval.

Refer to Section 4: HMIS Users Workgroup Responsibilities for details on the annual review and annual process.

SYSTEM CONFIGURATION

- The HMIS Lead will work with the HMIS vendor to ensure timely configuration of system updates required to implement HUD Data Standards.
- Any changes to data elements, user roles, or reporting functionality will be documented in system release notes shared with agencies.
- The HMIS Lead must test configuration changes before rollout.

DRAFT

Refer to Section 4: System Administrator Responsibilities for details on the annual review and annual process.

COMMUNICATION OF CHANGES

- The HMIS Lead will notify Participating Agencies of HUD Data Standards updates and related policy changes through written guidance, agency administrator briefings, and the HMIS Users Workgroup.
- Participating Agencies are responsible for ensuring internal dissemination of updates and maintaining compliance with revised standards.
- All HMIS users must complete any additional training modules required as part of the change implementation process.

IMPLEMENTATION TIMELINE

- The HMIS Lead will publish an implementation timeline for each major HUD Data Standards update, including deadlines for system changes, policy adoption, and training completion.
- Agencies must complete required updates and training within the established timeline to maintain compliance.

Failure to comply with required implementation timelines may result in corrective action under Section 10: Monitoring and Compliance. .

CONTINUOUS IMPROVEMENT

- Feedback on the implementation of changes will be collected from Participating Agencies through the HMIS Users Workgroup.
- Lessons learned from each change cycle will be documented and used to improve future change management processes.

13. TRAINING AND TECHNICAL ASSISTANCE

The Alliance, as HMIS Lead, is responsible for establishing training standards and providing technical assistance to ensure that all HMIS users and Agency Administrators maintain compliance with HUD requirements and CoC policies. Participating Agencies are responsible for ensuring that their staff complete required training and adhere to established standards.

USER TRAINING REQUIREMENTS

- Pre-Access Training: All new HMIS users must complete privacy, security, and data entry training before being issued an HMIS User ID.
- Annual Training: All HMIS users must complete annual Privacy and Security training and any additional modules required by the HMIS Lead or HUD.
- Role-Based Training: Users must complete training specific to their access role (e.g., data entry, reporting, administration).
- Agency-Led Training (By Exception): Participating Agencies may conduct their own HMIS training for internal staff only if pre-approved by the MWVHA Board of Directors.
    - Agency-led training must use curriculum and materials approved by MWVHA.
    - The Agency Administrator must ensure training content remains current with MWVHA's HMIS Policies & Procedures and HUD Data Standards
    - The Agency must provide verification of each User's training completion to the MWVHA HMIS Lead prior to activation or continued access.
    - MWVHA reserves the right to audit agency-led training at any time to ensure compliance.

DRAFT

- Documentation: Completion of training must be documented and kept on file by the HMIS Lead. Users who fail to complete training will have their HMIS access suspended until requirements are met.

TECHNICAL ASSISTANCE (TA) OFFERINGS

- The HMIS Lead will provide technical assistance to Participating Agencies on:
  - Data entry and reporting requirements.
  - Privacy, security, and confidentiality standards.
  - Data quality monitoring and error correction.
  - Compliance with HUD Data Standards and CoC policies.
- TA may be provided in various formats, including one-on-one support, webinars, group workshops, written guidance, and desk aids.
- Agencies experiencing repeated compliance or data quality issues may be required to participate in targeted TA as part of a corrective action plan.

Refer to Section 8: Data Collection and Quality for more information on Data Quality Standards.

Refer to Section 10: Monitoring and Compliance for more details on the requirements related to monitoring and compliance.

ENFORCEMENT

- Failure to complete required training or to participate in required technical assistance may result in suspension of user accounts, corrective action, or other enforcement measures as outlined in Section 10: Monitoring and Compliance.

14.GLOSSARY OF TERMS

Agency Agreement
A written agreement between the HMIS Lead and each Contributing HMIS Organization (CHO) outlining roles, responsibilities, and compliance expectations.

Annual Performance Report (APR)
A HUD-required report generated from HMIS data for each CoC-funded project. Used to evaluate performance and determine continued eligibility for funding.

Audit Trail
The automatic system record that logs all HMIS user activity, including logins, data entry, edits, and report runs.

Comparable Database
A secure database used by VSPs that meets HUD HMIS Data Standards and VAWA confidentiality rules. Must be capable of generating HUD-required reports.

Consolidated Annual Performance and Evaluation Report (CAPER)
A HUD-required report for ESG-funded projects that evaluates program outcomes based on HMIS data.

Contributing HMIS Organization (CHO)
Any agency or program that enters data into HMIS under a signed Participation Agreement.

DRAFT

Custom Reports
Specialized reports requested by agencies to analyze program outcomes, funding applications, or community planning.

Data Quality Plan
A CoC-adopted policy that defines standards for timeliness, completeness, and accuracy of HMIS data, as well as monitoring and corrective action procedures.

Data Quality Reports
Reports generated by the HMIS Lead to identify missing, incomplete, or inaccurate client records. Used for monitoring and corrective action.

Encryption
The process of encoding electronic data (such as HMIS records) to prevent unauthorized access.

Homeless Management Information System (HMIS)
The community-wide data system designated by the CoC to collect information about the characteristics and service needs of people experiencing homelessness and those at risk.

Housing Inventory Count (HIC)
An annual inventory of all beds and units dedicated to serving homeless individuals and families, reported to HUD along with the PIT Count.

Longitudinal Systems Analysis (LSA)
An annual system-level report generated from HMIS and submitted to HUD. Provides data for national analysis of homelessness trends.

Multi-CoC HMIS Governance Committee
A statewide or regional body that oversees HMIS governance across multiple CoCs to ensure consistency and compliance with HUD standards.

Personally Identifiable Information (PII)
Any information that can be used to identify a client, such as name, Social Security Number, date of birth, or address.

Point-in-Time (PIT) Count
A HUD-mandated count of sheltered and unsheltered homeless individuals on a single night in January. Data is entered into HMIS or collected by other approved methods.

Program-Specific Data Elements (PDEs)
Additional data required for some federal project types, such as income and sources, non-cash benefits, disabilities, health insurance, and housing move-in date.

Release of Information (ROI)
Written or electronic authorization by a client that specifies what personal information may be shared, with whom, and for what purpose.

System Performance Measures (SPMs)
A set of HUD-defined metrics that evaluate overall CoC performance, including length of time homeless, returns to homelessness, and employment/income growth.

DRAFT

Timeliness Standard
The requirement that client data (entry, exit, services) be entered into HMIS within a set timeframe (usually five business days).

Two-Factor Authentication (2FA)
An additional security measure requiring a second form of verification (e.g., code sent to a mobile device) when logging into HMIS.

Universal Data Elements (UDEs)
Baseline data elements required by HUD to be collected on every client, regardless of project type. Includes Name, Date of Birth, Gender, Race, Ethnicity, Veteran Status, and project entry/exit dates.

User ID and Password
A unique credential assigned to each HMIS user. Accounts may not be shared between staff.

Violence Against Women Act (VAWA) Confidentiality
Federal requirements that prohibit Victim Service Providers (VSPs) from entering client-identifying information into HMIS. Instead, VSPs must use a comparable database and follow strict confidentiality provisions.

DRAFT