CDSA- HMIS Policies & Procedures

Community-Wide HMIS Access, Privacy and Security

WellSky

Community Services

CDSA

Community Solutions

HMIS Lead Agency Contact
Angel Nelson – Information Specialist
114 S. Independence
Enid, OK 73701
580-242-6131
hmis@cdsaok.org

TABLE OF CONTENTS

CDSA HMIS Lead History

United Way of Ponca City held the HMIS grant and Lead Agency role for North Central Oklahoma CoC (OK-500) since 2002. By 2006, Northeast Oklahoma (OK-505) and Southeastern Oklahoma Regional (OK-507) CoCs joined the North Central HMIS system. United Way of Ponca City staff supported all three CoCs as HMIS Lead Agency and Administrator. In 2011, United Way of Ponca City merged its HMIS data from their ServicePoint system onto the ServicePoint system operated by Tulsa's Community Service Council (tulsalive). In 2019, CDSA, Inc. agreed to assume this role and OK-500, OK-505, and OK-507 each unanimously voted in their June 2019 CoC Board Meetings for CDSA, Inc. to serve as a multi-CoC HMIS Lead Agency for the three CoCs (OK-500, OK-505, and OK-507). In March 2024, OK-505 voted to terminate their agreement with CDSA, name themselves as HMIS Lead Agency for OK-505, and to contract with Information Services Oklahoma, LLC (ISOK, LLC) . Currently, CDSA, Inc. continues to implement a Multi-CoC Implementation model by serving as HMIS Lead Agency for OK-500 and OK-507. In 2024, CDSA completed a systems revision to better serve as HMIS Lead. This revision ensures HUD compliance while using new tools and guidance to support OK-500 and OK-507 while they increase their capacity to eliminate homelessness.

Common HMIS Acronyms

Term	Acronym	Brief Definition
Agency Administrator Agreement		The document each Agency Administrator signs agreeing to perform the Agency Administrator responsibilities.
Agency Participation Agreement		The Agreement between all participating agencies and CDSA that specifies the rights and responsibilities of CDSA and participating agencies.
Agency Privacy Policy		Each Participating Agency must have a Privacy Policy that protects the privacy and confidentiality of their Clients.
Audit Trail		An extensive auditing system with ***Community Services*** software that monitors, records and reports on what valid users of HMIS are doing within the database.
Authentication		The process by which users validate their identity. In ***Community Services*** this entails establishing a unique User Name and Password for each user license.
Comparable Database		A database used by a victim service provider that collects Client-level data over time and generates unduplicated aggregate reports based on the data, in accordance with regulations.
Confidentiality		A Client's right to privacy of the personal information that is communicated in confidence to a case manager (or other agency staff) that is stored within the HMIS.

Continuum of Care	CoC	The group organized to carry out the responsibilities required under this part and that is composed of representatives of organizations, including nonprofit homeless service providers, victim service providers, faith-based organizations, governments, businesses, advocates, public housing agencies, school districts, social service providers, mental health agencies, hospitals, universities, affordable housing developers, law enforcement, organizations that serve homeless and formerly homeless veterans, and homeless and formerly homeless persons to the extent these groups are represented within the geographic area and are available to participate.
Covered Homeless Organization	CHO	Any organization (including its employees, volunteers, affiliates, contractors, and associates) that records, uses or processes protected personal information on Clients for an HMIS.
Encryption		Conversion of plain text into encrypted data by scrambling it using a secret code that masks the meaning of the data to any unauthorized viewer. Computers encrypt data by using algorithms or formulas. Encrypted data are not readable unless they are converted back into plain text via decryption.
Homeless Management Information System	HMIS	The information system designated by the Continuum of Care to comply with the HMIS requirements prescribed by HUD. The HMIS is also the primary reporting tool for HUD CoC homeless assistance program grants as well as other public funds related to homelessness.
HMIS Lead Agency		An entity designated by the CoC in accordance with the regulations to operate the CoC's HMIS on its behalf. (CDSA for OK-500 and OK-507)
HMIS User Agreement & Code of Ethics		The document each HMIS User signs agreeing to the HMIS standards of conduct and operating policies and procedures.
Housing Inventory Chart	HIC	HUD requires each CoC to annually submit a chart that lists all homeless residential programs (both HMIS and non-participating), specifying the type and number of beds/units available to homeless persons within the geographic area covered by the CoC. The HIC information is entered into Provider Administration section in HMIS.
Length of Stay	LOS	The number of days between the beginning of services and the end of services. It is calculated using entry and exit dates or shelter stay dates. The HMIS offer calculations for discrete stays as well as the total stays across multiple sheltering events.
Longitudinal Data Analysis	LSA	A report that provides the HMIS data used to complete the AHAR, or Annual Homeless Assessment Report, submitted to Congress annually and to the Stella Performance. The LSA includes detail about households' system use that will allow CoCs to understand lengths of homelessness, exits to permanent housing, And returns for each household type.
Participating Agency		Organizations that participate in HMIS; also referred to as "Agency".
Personal Protected Information		PPI Information that identifies Clients contained within the database. Examples of confidential data include: social security number, name, address, or any other information that can be used to identify a Client.

Point in Time Count	PIT	An annual count of sheltered and unsheltered homeless persons during the last week in January that is required by HUD for all CoCs. Every other year, that count also includes an “unsheltered” / street count.
Release of Information	ROI	A signed (paper) document giving informed Client consent for sharing Client data. ROIs may be required for certain projects so the funder can monitor the Client files. ROIs may be required by the Agency to share data to another Agency.
Stella Performance	Stella P	A strategy and analysis tool that helps the CoC understand how the system is performing and models what an optimized system would look like that fully addresses homelessness in the CoC geographic area. Stella P provides dynamic visuals of CoCs’ Longitudinal Systems Analysis (LSA) data to show how households move through the homeless system, and to highlight outcome disparities. It looks at the system’s past performance to see where the community can make future improvements. Raw, de-identified data from HMIS is used for Stella P analysis.
System Performance Measures	SPM	7 HUD measures which provide a more complete picture of how well the community is preventing and ending homelessness. The number of homeless persons measure directly assesses the CoC’s progress toward eliminating homelessness by counting the number of people experiencing homelessness both at a point in time and over the course of a year. The six other measures help the community understand how well they are reducing the number of people who become homeless and helping people become quickly and stably housed. Raw, de-identified data from HMIS is used for Stella P analysis.

HMIS Overview

The Homeless Management Information System (HMIS) is a database which allows authorized personnel at housing and social service agencies to enter, track, and report information on the Clients they serve. HMIS provides opportunities for service providers that serve the same Client to operate with a single case plan, reducing the amount of time spent in documentation activities and ensuring that care is coordinated, and meets the reporting requirements for the
U.S. Department of Housing and Urban Development (HUD) and other funders.

HMIS utilizes ***Community Services*** (formerly ServicePoint) developed by WellSky. ***Community Services*** is a client information system that provides a standardized assessment of participant demographics, creates individualized service plans, and records the use of housing and services. OK-500 and OK-507 will use this information to better understand the use of services, identify gaps in the local system of services, and develop outcome and performance measures.

Involvement in HMIS will allow service providers to generate automated reports which can aid in the development and evaluation of programming. At a community level, HMIS will provide aggregated data across the entire homeless service continuum for use in the annual Continuum of Care funding application and city and county consolidated plans. Findings can also be used to inform policy decisions aimed at addressing and ending poverty and homelessness at the local, state, and federal levels. Finally, and most importantly, HMIS will ease the process of securing services for individuals and families who are at-risk or experiencing homelessness in OK-500 and OK-507. A more complete list of the potential benefits of HMIS is available on the page that follows.

This document provides information about HMIS staffing, technology, and participation requirements, as well as an overview of policies, procedures, and standards that govern its operation especially regarding confidentiality, security, and data expectations. Copies of all necessary supporting documents are also included in this manual as well as a glossary of commonly-used terms.

Program Types in HMIS

Program Types		HUD defines 9 basic Program Types:
Emergency Shelter	ES	A facility, the primary purpose of which is to provide a temporary shelter for people experiencing homelessness and which does not require occupants to sign leases or occupancy agreements
Transitional Housing	TH	Provides homeless individuals and families with the interim stability and support to successfully move to and maintain permanent housing. Transitional housing may be used to cover the costs of up to 24 months of housing with accompanying supportive services.
Permanent Supportive Housing	PSH	Permanent housing with indefinite leasing or rental assistance paired with supportive services to assist homeless persons with a disability or families with an adult or child member with a disability achieve housing stability.
Permanent Housing	PH	Community-based housing without a designated length of stay in which formerly homeless individuals and families live as independently as possible.
Rapid Rehousing	RRH	Permanent housing type which emphasizes housing search and relocation services paired with short- and medium-term rental assistance to move homeless persons and families (with or without a disability) as rapidly as possible into permanent housing.
Homeless Prevention	HP	Housing relocation and stabilization services as well as short- and medium-term rental assistance to prevent an individual or family from becoming homeless
Safe Haven	SH	Form of supportive housing that serves hard-to-reach homeless persons with severe mental illness who come primarily from the streets and have been unable or unwilling to participate in housing or supportive services.
Street Outreach Program	SO	A program that seeks to reach unsheltered people experiencing homelessness to connect them with emergency shelter, housing and other critical services.
Supportive Services Only Program	SSO	A program that serves homeless persons that does not directly provide shelter or housing. These programs often provide case management or other forms of supports in an office, at the household’s home, or in a shelter.

Benefits of HMIS

For people experiencing poverty or homelessness	For social service providers	For the community
Makes it possible to maintain intake information over time so the number of times a Client repeats their story to providers is reduced.	Provides real-time information about needs and available services for Clients.	Helps the community to define and understand the extent of poverty and homelessness throughout Lane County.
Offers an opportunity to conduct intakes and life histories once; illustrating that service providers consider the Client's time valuable and ensuring Client dignity.	Assures confidentiality by keeping information in a secured system.	Provides greater focus for staff and financial resources to the geographical areas, agencies, and programs where services are needed most.
Makes it possible to coordinate multiple services and streamline referrals. This will help to reduce Client waiting time.	Decreases duplicative Client intakes and assessments. Reduces time required to conduct intakes and assessments.	Allows for better evaluation of the effectiveness of specific interventions, programs, and services.
	Tracks Client outcomes and provides a Client history.	Offers local, state, and federal legislators' data and information about the population served
	Generates data reports for local use and to meet funding requirements.	Makes it possible to meet all federal reporting requirements.
	Facilitates the coordination of services internally and externally with other agencies and programs.	
	Provides access to a community-wide database of service providers and allows agency staff to easily select a referral agency.	

HMIS Roles & Responsibilities

Wellsky Client Services	Responsible for the delivery of Internet-based Client assessments and reporting features. Wellsky will provide secure, on-going access to its suite of applications in Community Services. Wellsky will also provide information about any system modifications and/or upgrades.
Continuum of Care	Must designate a single information system as the official HMIS software for the geographic area. Designate an HMIS lead to operate the HMIS Develop a governance charter which at minimum includes: A requirement that the HMIS Lead enter written HMIS Participation Agreements with each participating agency The participation fee (if any) charged by the HMIS Maintain documentation evidencing compliance with regulations and with the governance charter Review, revise and approve the policies and plans required by HUD regulation and any notices issued from time to time.
Community Development Support Association, Inc. (CDSA)	The HMIS Lead Agency. The HMIS Lead Agency is responsible for: Ensuring the operation of and consistent participation by recipients of funds from the Emergency Solutions Grant Program and from other programs authorized by Title IV of the McKinney-Vento Act. Developing written policies and procedures in accordance with regulations. Executing a written HMIS Participation Agreement with each CHO. Serving as the applicant to HUD for grant funds to be used for HMIS. Monitoring and enforcing compliance by all CHO's. Submitting a security plan, data quality plan and privacy policy to the CoC for approval within six months of any changes to the regulations. Reviewing and updating HMIS documents at least annually that incorporates feedback from the HMIS Advisory Committee and CoC approval. CDSA will secure funding for the HMIS and provide organizational oversight through the OK-500 Lived Experience and the HMIS Advisory Collaboratives. CDSA will also provide regular staffing for the project.
HMIS Joint Advisory Committee (HAC)	Responsible for developing and reviewing all system-wide policies and procedures for HMIS. In selecting participants for this committee, CDSA will attempt to secure and maintain representation from each: Data/Analytic professionals Person(s) with Lived Experience Continuum of Care municipalities Exceptional HMIS Users The HAC will provide input on an on-going basis for the local HMIS project. The Committee will share its recommendations with the CoC Board on the key issues that follow: Determining guiding principles for HMIS Selecting data elements to be collected in addition to HUD requirements by participating agencies Defining parameters for the release of aggregated HMIS data Evaluating HMIS compliance with HUD data and technical standards Reviewing the HMIS-related performance of the system and of participating agencies Reviewing the adherence to local policies and procedures; Reviewing Security Incident Reports Addressing issues that arise from use of HMIS including, but not limited to, Client grievances and policy adjustments

HMIS System Administrator (System Admin)	The HMIS System Administrator is a CDSA staff person responsible for the implementation and coordination of the local HMIS. The administrator will be the primary contact for HMIS participating agencies and HMIS Agency Administrators Responsibilities include: Orienting prospective HMIS participants to system Maintaining a list of agency contacts and HMIS participants Providing oversight on all contractual agreements Assessing agency readiness for HMIS Developing training materials Preparing regular trainings for Agency Administrators Authorizing access to the HMIS (Set-Up) Developing Client assessment tools not already included Providing basic technical assistance activities to participating agencies Monitoring, reporting, and resolving access control violations
HMIS Information Specialist	The HMIS Information Specialist is a CDSA staff person responsible for HMIS analytics and reporting. The HMIS Information Specialist is the CoC designated HMIS Lead. The analyst will be the primary contact for CDSA the HMIS Advisory Board, and the CoC Governing Board. Documenting database and policy/procedure changes Developing and evaluating performance objectives Updating HMIS training materials Auditing HMIS usage system-wide Developing reports and queries for Continuum of Care Presenting research findings to community stakeholders Coordinating regular user-group meetings Communicating with participating agencies/larger community Representing the CoC as the HMIS Lead
HMIS Agency Administrator	The HMIS Agency Administrator is an Agency staff person who serves as the agency contact for the project and will facilitate access to the HMIS at the user organizational level. Each Agency Administrator, with the support of agency leadership, will be responsible for: Participating in HMIS readiness assessment Identifying HMIS users and providing or facilitating access to training Granting HMIS access staff members that have received training and demonstrated proficiency in system use and understanding of policies and procedures Monitoring staff compliance with standards of Client consent and confidentiality and system security Enforcing business controls and practices to ensure organizational adherence to policies and procedures including detecting and responding to violations Providing on-site support for the generation of agency reports and managing user licenses Running reports in ***Community Services*** and the ***Community Services*** reporting tool for Agency Management and Agency Users Ensuring stability in the agency Internet connection either directly or in communication with a technician Notifying users about interruptions in service.

HMIS Users	HMIS Users are Agency staff responsible for entering Client data into the system as well as identifying needs and concerns regarding HMIS to their Agency Administrator. HMIS Users will be responsible for: Being aware of the confidential nature of data and taking appropriate measures to prevent any unauthorized disclosure of Client information Accurate and timely data entry Complying with all local HMIS policies and procedures Reporting security violations to their HMIS Agency Administrator Users are also responsible for their own actions or any actions undertaken with their usernames and passwords.
HMIS Participating Agency and Partner Agencies	A Participating Agency has signed the OK HMIS Agency Participation Agreement agreeing to adhere to the policies set forth in the participation agreement and this agreement. Partner Agencies are other Participating Agencies using this implementation of HMIS.

Policies and Procedures

Participation

All social service providers assisting people experiencing poverty or homelessness are ***strongly encouraged*** to participate. Participation in HMIS is mandatory as required by funder(s), such as HUD, HHS, and ESG.

In order to participate in HMIS, providers must agree to each of the following:

Agency Participation Agreement: Agencies are required to sign a participation agreement stating their commitment to adhere to the policies and procedures for effective use of HMIS and proper collaboration with the respective CoC. A copy of the Agency Agreement is available in the Supporting Documents section of this manual and on the CDSA website, www.cdsaok.org.

Identification of HMIS Agency Administrator(s): Agencies will designate one or more key staff persons to serve as HMIS Agency Administrator(s). The Agency Administrator is the primary liaison with the System Administrator and serves as the Agency contact for the project and will facilitate access to the HMIS at the user organization level. The Agency Administrator is responsible for relaying all HMIS information from CDSA staff to Agency management and users.

Training: HMIS Agency Administrators will be responsible for identifying HMIS Users and coordinating initial and any subsequent training sessions. Each new User must complete training prior to gaining access to HMIS.

Training Materials

CDSA is responsible for HMIS training materials.

HMIS Agency Administrator Group Meetings: Agencies must agree to send at least one representative to attend bi-monthly Agency Administrator meetings. This representative is responsible for disseminating information to other agency HMIS Users.

Client Consent: Agencies will post the Privacy Sign in all public areas of the facility as well as intake rooms and other locations Clients use. Agencies will read from a Privacy Script to the head of household at any time data are collected for intake (entry) assessments.

Data Collection: Agencies agree to collect Client information on all HUD- and locally- required data elements. HUD-required elements are identified through Data and Technical Standards. Local elements will be established by the HMIS Advisory Committee.

Equipment, System Requirements, Software Information and Licensure

The following are the minimum requirements for operating ***Community Services*** (as recommended by the vendor, Wellsky.

Memory

- If Win7 – 4 Gig RAM recommended, (2 Gig minimum)
- If Vista – 4 Gig RAM recommended, (2 Gig minimum)
- If XP – 2 Gig RAM recommended, (1 Gig minimum)
- Up-to-Date Anti-Virus Protection

Other recommendations for maximize the performance of HMIS:

Browser Recommendations:

- Google Chrome, version 11.0.696.65 or above (Recommended)
- Microsoft Internet Explorer, version 7 or above.
- Mozilla Firefox, version 3.5 to 4 (soon to be 3.5, 4, 5 and beyond)
- Apple Safari, version 4 or 5

Internet Connection: Broadband (recommended) or LAN connection.
Monitor: Screen Display - 1024 by 768 (XGA) or higher (1280x768 strongly advised)
Processor: Avoid using single-core CPUs

System Availability: The HMIS is available 24 hours a day, 7 days a week, 52 weeks a year except for scheduled system upgrades and routine maintenance. In the event of planned downtime, the HMIS Administrator will inform Agency Administrators via email.

If there is unexpected service interruption, the HMIS Administrator will contact the HMIS Agency Administrators to inform them of the cause and possible duration of the service interruption. Contact will be made via email.

Technical Support: The HMIS Administrator will provide system support by phone, email, computer shadowing, and/or in-person consultations. The HMIS Agency Administrator should act as the first level of contact when a system problem arises and should determine if the problem requires immediate rectification. If the HMIS Agency Administrator cannot resolve the problem, the Agency Administrator should contact HMIS System Administrator. HMIS System Administrator will respond to the call as soon as possible.

Participating agencies are responsible for their own computer hardware and Internet connections, thus will be responsible for accessing technical following their Agency's protocols.

Data Ownership: Participating agencies are the owners of all Client data collected and stored within HMIS. This data is protected and secured by the policies, technologies, and security protocols held in place. All participating Agencies must take full responsibility of ownership and confidentiality protection of any and all data that is collected at their agency and/or downloaded from HMIS.

Privacy and Data Sharing Plan

There are two levels of data sharing in the HMIS. The CoC is considered an "open" system where participating agencies share all data relevant to providing housing and services to the persons experiencing poverty or homeless with Client consent. Sharing data will reduce the amount of time that Agencies and Clients will need to spend at intake repeating the same information that has already been shared with multiple providers in the community and will allow for better coordination of services for Clients in the homeless system. Sharing data will also support the CoC's goal of designing a centralized point of entry using a common assessment tool (located in HMIS) that will ensure Clients are being directed to the housing and services that best meet their household's needs.

Level 1 Data Elements: Name, Security Number, Veteran Status, and Year of Birth. These elements will prevent duplication of records in the system.

Level 2 Data Elements: Data collected through the assessments (Entry/Exit entries, reviews, and exits).
Agency defaults within the HMIS will be set to "open" except for:

- Child head-of-household households
- Clients requesting entry/exit or service transactions/needs not be shared to other Participating Agencies.

The User entering the client's data into HMIS and the Agency Administrator for this project are responsible for identifying records which need the visibility reduced.

No Share Policy:

- If the Client rejects the sharing plan, agency staff is responsible for closing the record in HMIS to reduce the visibility of the Entry/Exit.
- Agency staff must verbally inform the Client when services will be, or could be, reduced or otherwise not available if the Client elects not to share.
- Clients' decision to share or not share shall be voluntary.
- Clients who choose not to authorize sharing of information must be clearly informed if they could be denied services for which they would otherwise be eligible.
- Client records shall not be "closed" (visibility changed) except by the System Administrator.
- Client Entry/Exit assessments can be closed by the Agency Administrator at the Agency level at the request of the Client.
- Restricted information, including progress notes and psychotherapy notes, about the diagnosis, treatment, or referrals related to a mental health disorder, drug or alcohol disorder, HIV/AIDS, and domestic violence concerns (excluding status) shall not be shared with other participating agencies without the Client's written, informed consent as documented on the Agency's own Release of Information Form.
  Sharing of the above restricted information is not covered under the HMIS Client Consent process.
- If a Client has previously given permission to share information with multiple agencies, beyond basic identifying information and non-restricted service transactions, and then chooses to revoke that permission, the record will be locked by the agency from future sharing. Record prior to the revocation will remain shared.

Exceptions: Client PII and contact information can be shared to non-participating organizations when there is a demonstrable health or safety situation or event.

- The Client must be in shelter or housing and be at risk of discharge or eviction or the client must be on the waitlist for a shelter or housing project that uses HMIS.
- The Provider working with the client may be asked to provide the HMIS Lead with specific events or details from which a health or safety concern was determined.
- The Provider must track the referral in HMIS in Case Notes or as a Referral Transaction. The documentation must include:
    - Date the client data was shared

    - Organization, staff name, and contact information of who received the information
    - Organization, staff name, and contact information of who shared the information
- The referral recipient must be a licensed health care provider, behavioral health provider or an Aging and People with Disabilities (APD) program.

Client Privacy Policy

The Agency will use various tools to inform Clients of data collection practices, reasons, and options.

Client Informed and Verbal Consent

Participating agencies are required to inform Clients that the Agency uses HMIS for tracking services the Agency provides. The Agency ***does not*** need consent to track Clients and services in HMIS. The agency ***does*** need consent from the Client to allow the information to be shared with the other Participating Agencies using this HMIS. It is assumed that, by requesting services from the Agency, the Client consents to share information to the other Agencies in the HMIS. Verbal consent will be determined using these two methods:

- Posted Privacy Signs in the lobbies and Client intake areas in languages typically used by the Client
- The Privacy Script will be read to the Client by the User or other Agency staff at project entry (entry/exit entry assessment data collection) in the language of the Client

Reducing the visibility of the Entry/Exit to the Agency level means that the Entry/Exits and Service Transactions cannot be seen by other Agencies. It also means that the data entered into the assessment will not roll forward to new assessments created by other Agencies. In some cases, such as projects shared between Agencies and Coordinated Entry, the Client will not be able to receive services without allowing the Entry/Exit to be visible between Participating Agencies.

If the Client is unwilling for their Name or Date of Birth and other Personally Identifiable Information (PII) to be entered into HMIS or the Agency staff believe the Client should not have PII entered into the system for safety concerns, then the Agency Administrator will contract theSystem Administrator who will remove the PII from the record. Changes include:

Data Element	Protected Data Element
Client First Name	Initial of First Name
Client Middle Name	“Anonymous”
Client Last Name	Head of Household Client ID Number
Date of Birth	01/01/YYYY
Date of Birth DQ	Refused
Social Security Number	Null
SSN DQ	Refused

The agency is required to keep a document of the Client's actual PII and the Client ID in HMIS. This document may be monitored if required by funders.

These requests are expected to be rare. If the Agency has more than two (2) households within a twelve month period requesting PII removal from HMIS, the System Administrator may require a training for all Agency Users.

The Agency is responsible for ensuring that this procedure takes place at the initial contact for each Client. In instances where the Client speaks a language other than English or seems to have difficulty understanding, it is the responsibility of the Agency to seek ways to remove language access barriers and make sure consent is informed.

The Agency must agree not to release any confidential information received via HMIS to any organization or individual outside of the participating agencies without proper written consent.

Definitions

Privacy Sign	Brief notice about HMIS and Client privacy protections, which must be posted where Clients are served.
Privacy Script	At entry into the program (***Community Services*** Entry/Exit entry assessment), the Agency staff will read verbatim a verbal explanation of both the HMIS project and the terms of consent. The script (CDSA HMIS Privacy Script) is a living document, to be frequently reviewed by the CDSA Agency Admin Workgroup.
Privacy Protection Notice	A notice detailing all privacy protections should be made available to Clients upon request.
Wellsky ROI	HMIS uses an informed consent model to share data in the system between participating agencies. CDSA HMIS uses the Wellsky ***Community Services*** Release of Information function to document that the client has accepted the terms if the Privacy Script which is read or shown to every household.
Revocation of Consent	If a Client chooses to revoke the Consent to Share, it should be understood that only data going forward will not be shared. Historical data will remain shared.
Use of Anonymous Client Feature	This feature is not used in CDSA HMIS as it is not reportable.

CDSA HMIS Security Plan

Wellsky Security Responsibilities

Wellsky's security responsibilities are outlined in the Wellsky Security Client Data document on the North Central Oklahoma website. The document outlines the measures taken by WellSky to secure all Client data on the ***Community Services*** site. The steps and precautions taken to ensure that data is stored and transmitted securely are divided into six main sections – Access Security, Site Security, Network Security, Disaster Recovery, HIPAA Compliance, and Unauthorized Access.

HMIS Lead Agency and Participating Agency Security Responsibilities

All Agencies (HMIS Lead Agencies and CHOs) must assign the duties of the Security Officer to the Agency or System Administrator. In this role, the Administrators are responsible for:

- Insuring that all staff using the HMIS have completed the required privacy & security training(s).
- Insuring the removal of HMIS licenses when a staff person leaves the organization
- Revising Users' HMIS access levels as job responsibilities change.
- Reporting any security or privacy incidents to the HMIS administrator. The System Administrator investigates the incident including running applicable audit reports. If the System Administrator determines that a breach has occurred and/or the staff involved violated privacy or security guidelines, the System Administrator will report to the chair of the appropriate CoC Board. A Corrective Action Plan will be implemented for the agency. Components of the Corrective Action Plan must include at minimum supervision and retraining. It may also include temporary suspension of HMIS license(s), Client notification if a breach has occurred, and any appropriate legal action.

CDSA conducts routine audits of participating Agencies to insure compliance with the Standard Operating Procedures Manual. CDSA will use a checklist to guide the inspection and make recommendations for corrective actions.

- Agencies are required to maintain a culture that supports privacy.
- Staff does not discuss Client information in the presence of others without a need to know.
- Staff eliminates unique Client identifiers before releasing data to the public.
- Staff does not use any Client PII (including client name) in email or other electronic communication. Any screenshots taken from HMIS must have all PII removed or obscured.
- The Agency configures workspaces for intake that supports privacy of Client interaction and data entry.
- User accounts and passwords are not shared between users, or visible for others to see.
- Program staff is educated to not save reports with Client identifying data on portable media as evidenced through written training procedures or meeting minutes.
- All staff using the System must complete the required privacy & security training(s) annually. Certificates documenting completion of training must be stored at the Agency for review upon audit.
- Victim Service Providers may be prohibited from entering Client level data in HMIS. Providers that receive McKinney-Vento funding must maintain a comparable database to be in compliance with grant contracts.

Physical Security: Passwords are required to access individual workstations. Any raw data or system information is stored in locked cabinets to maintain confidentiality and security.

System Access Monitoring: Wellsky ***Community Services*** automatically tracks and records access to every Client record by use, date, and time of access. The System Administrator will monitor access to HMIS by regularly reviewing user access frequency and deactivate licenses when users no longer require access.

The System Administrator will confirm (through the monitoring process) that the Agency provides HMIS workstations that:

- Have and use a hardware or software firewall.
- Have and use updated virus/spy protection software.
- Have and use screens saver and require a password to re-activate.
- Have screens positioned so that data is not visible to others; (i.e. – other staff, Clients, etc. who are in the immediate area).
- Workstations do not have user names and/or passwords posted in visible and/or accessible locations.

User Authentication: HMIS will only be accessed with a valid username and password combination, which is encrypted via SSL for Internet transmission to prevent theft. If a user enters an invalid password three consecutive times, HMIS automatically marks them inactive. Users can securely reset their own password if forgotten or if they exceeded the maximum number of login attempts.

Administration and System-wide Data: The HMIS System Administrator and HMIS Analyst have full access to HMIS. The System Administrator and HMIS Analyst can add, edit, and delete users, agencies, and programs and reset passwords. Access to system-wide data will be granted based upon need to access the data. The HMIS System Administrator is responsible and accountable for the work done under system information and personal identifiers.

User Access: Users will be able to view the data entered by their agency and from users of all participating agencies with the exception of data from Clients who do not agree to share data collected at other participating agencies in the system.

Background Checks: Criminal background checks must be completed on System Administrators.

Raw Data: Users who utilize Report Writer and/or ART have the ability to download and save Client level data onto their local computer. Once this information has been downloaded from HMIS in raw format to an agency's computer, the data becomes the responsibility of the Agency.

Policies Restricting: Each HMIS participating agency must establish internal policies on access to data protocols. These policies should include who has access, for what purpose, how they can transmit this information, and address issues include storage, transmission, and disposal of data downloaded from HMIS.

Client Paper Record Protection: Partner agencies must establish procedures to handle Client paper records associated with HMIS such as copies of Intake Assessments. Procedures that must be addressed include:

- Identifying which staff has access to Client paper records and for what purpose;
- Allowing staff access only to the records of Clients whom they work with or for data entry purposes;
- How and where Client paper records are stored;
- Length of Client paper record storage and disposal procedures; and
- Disclosure of information contained in Client paper records.

Access Monitoring: The Agency Administrator will be responsible for monitoring all User access within their Agency. Any violations or exceptions should be documented and forwarded to the System Administrator immediately.

All suspected data, system security, and/or confidentiality violations will incur immediate user suspension from the HMIS until the situation is effectively resolved. Serious or repeated violation by users of the system may result in the suspension or revocation of an agency's access to HMIS.

Any user/agency found to be in violation of data, system security, and/or confidentiality protocols will be sanctioned accordingly. Recommended sanctions may include but, are not limited to, a formal letter of reprimand, suspension of system privileges, revocation of system privileges, termination of employment, loss of funding, and criminal prosecution.

Security Incidents:

A security incident is defined as any occurrence that adversely affects or has the potential to adversely affect the integrity and/or confidentiality of the information contained within HMIS or its operation.

Security incidents can be categorized as the following:

Category	Definition
Data or file extraction	Unauthorized, electronic removal of information from HMIS.
Introduction of malicious code or virus	Intentional or unintentional, unauthorized introduction of malicious code or virus onto the HMIS or agency
Misrepresentation of data	Intentional or unintentional, misrepresentation of Client/computer equipment.
Attempts to modify passwords or access rights	Intentional or unintentional attempt to modify HMIS user passwords or access rights.
Compromised or lost password	A compromise in a password occurs when staff believes that an individual other than the one to which the password is assigned becomes aware of the password. Sharing a license is considered a compromise.
Theft of HMIS equipment or media	This includes stolen PCs, devices, or media that may contain Client information.
Dissemination of protected Client information from HMIS in electronic or paper form	Intentional or unintentional, unauthorized dissemination of Client information in an electronic format. This includes sending email or a FAX to an unintended recipient.

Security Incident Documentation: All security incidents must immediately be reported to the System Administrator via phone call. The System Administrator will provide direction as needed to the individual(s) responding to the security incident and to evaluate the necessity of mobilizing additional resources. The System Administrator is also responsible for ensuring that immediate action is taken to protect the security and integrity of the HMIS and Client data.

After the security incident, the Agency Administrator must complete a written Security Incident Report, the CDSA HMIS Security Incident Report, as soon as possible and forward it to the System Administrator. The purpose of the report is to provide subsequent readers with an accurate image of the security incident through written documentation.

The report should be written in a clear, concise, and specific manner and should focus on the facts and events that occurred immediately prior to the incident, the incident itself, and the events that occurred immediately after the incident.

In addition to the above items, the report should include:

Parties involved including each staff member’s full name;

- A summary of each party’s actions;
- Time and location of the incident; and
- Observations of any environmental characteristics that may have contributed to the incident.

The System Administrator will take responsibility for reporting the incident to the OK-500 Lead Agency Executive Director or OK-507 Lead Agency Executive Director, HMIS Advisory Committee, and when appropriate, law enforcement officials.

If the security incident occurred at CDSA, it should be reported to the CDSA Executive Director who will assign the appropriate staff to investigate and report to the HMIS Advisory Committee.

Review of Security Incidents: Severe security incidents will be reviewed at the next regularly scheduled meeting of the HMIS Advisory Committee to ascertain if the incident could have been avoided or the impact minimized. Each incident will be scrutinized to determine the appropriateness of staff actions and protocols. Recommendations about the need for additional resources, staff training, security modifications, and protocols will also be noted.

More specifically, the HMIS Joint Advisory Committee will:

- Evaluate the timeliness, thoroughness, and appropriateness of the staff member’s response to the security incident;
- Ascertain if the security incident could have been prevented;

- Recommend corrective actions, if warranted;
- Evaluate security incidents for trends and patterns;
- Monitor the agency's compliance with the security policies and protocols;
- Monitor the implementation of any preventative or corrective action; and
- Recommend changes to the CoC Board regarding policies, procedures and practices, and working agreements that will reduce the likelihood that similar security incidents would occur.

An aggregate report of security incidents will be compiled by the System Administrator on a quarterly basis for review by the Data Quality Collaborative. At minimum, these incidents will be analyzed by type of incident, location, employee/organizational involvement, time and date.
Records of security incidents will be maintained by the System Administrator.

On-Going Review of Security Measures: The System Administrator and HMIS Advisory Committee will be responsible for providing on-going monitoring of agency compliance with appropriate procedures. This monitoring will include review of security policy and procedures and will occur on an annual basis.

Access to HMIS

Access Control: Access to HMIS will be controlled based on need. Need exists only for those administrators, program staff, volunteers, or designated personnel who work directly with Clients, who have data entry responsibilities or who have reporting responsibilities.

Access is controlled through user identification and authentication. Users are responsible and accountable for work done under their personal identifiers. Security violations will be monitored, reported and resolved. An agency or an individual user's access may be suspended or revoked for suspected or actual violation of the security protocols.

Passwords: Passwords are automatically generated by the HMIS when a new user is created or if a password is forgotten and needs to be reset. The Agency Administrator will communicate the system-generated password to each new User. The System Administrator will communicate the password to a new Agency Administrator.

Each user will be required to change the password the first time they log onto the HMIS. The password is alphanumeric and case sensitive. Passwords must be 8-50 characters long with a mix of numbers, special characters, and upper and lower case letters. Passwords are the individual's responsibility and users cannot share passwords under any even with staff members at their own agency. Passwords should not be easily guessed or found in any dictionary. They should be securely stored and inaccessible to other persons.

Passwords expire every 90 days. A password cannot be re-used until one entirely different password selection has expired.

Access Levels: User accounts can be created and deleted by the HMIS Agency Administrator or System Administrator. User access levels will be directly related to the user's job responsibilities and need for access to HMIS data.

Below is a list of "Access Levels" and chart of activity designations within the HMIS.

Title	Fee	Description
Resource Specialist I	YES	Resource Specialist I users are limited to the ResourcePoint module. This allows users to search for area providers and organizations and view their details. These users have no access to Client or service records. A Resource Specialist cannot modify or delete data. *Agencies must purchase Resource Specialist I licenses from CDSA.*
Resource Specialist II	YES	Resource Specialist II users have access to ResourcePoint. These users are also considered agency-level I&R specialists who update their own organization's information. To perform these tasks, they also have access to Admin Providers and Agency Newsflash. Agencies must purchase Resource Specialist I licenses from CDSA.
Resource Specialist III	N/A	Same as Resource Specialist II, but also includes access to System Newsflash and limited range of reports. *CDSA level users only.*
Volunteer	NO	Volunteers have access to ResourcePoint. These users can also view basic demographic information about Clients on the Profile screen, but they are restricted from viewing other assessments. A volunteer can create new Client records, make referrals, or check Clients in and out of shelters. Administrators often assign this user level to individuals who complete Client intakes and refer Clients to agency staff or a case manager. In order to perform these tasks, volunteers have access to some areas of ClientPoint.
Agency Staff	NO	Agency Staff users have access to ResourcePoint. These users also have limited access to ClientPoint, including access to service records and Clients' basic demographic data on the Profile screen. Agency Staff cannot view other assessments or case plan records. Agency Staff can also add news items to Agency Newsflash.
Case Manager I, II and III	NO	Case Managers have access to all ***Community Services*** features except those needed to run audit reports and features found under the Admin tab. They have access to all screens within ClientPoint, including assessments and service records. Case Manager II users can also create/edit Client infractions if given access by an Agency Administrator or above. Case Manager III users have the added ability to see data down their provider's tree like an Agency Admin.
Agency Administrator	NO	Agency administrators have access to all ***Community Services*** features, including agency level administrative functions. These users can remove users from their organization, as well as edit their organization's data. They also have full reporting access with the exception of two reports: Duplicate Client Report and the LSA Export. Agency Admins cannot access the following administrative functions: Assessment Administration, Direct Access to Admin>Groups, Picklist Data, Admin>Users>Licenses, or System Preferences.

		Agency Administrators can delete Clients that were created by organizations within their organizational tree. They shall not, however, delete Clients who are shared across organizational trees. Additionally, Agency Admins can delete needs and services created within their own organizational tree, unless the needs and services are for a shared Client. They shall not modify or delete needs, services, or E/E assessments belonging to other Agencies. An Agency Admin shall not delete or modify a Provider through Provider Admin unless given specific instructions from the System Administrator. Agency Admins have ART View licenses and are responsible for pulling all reports for the Agency
Executive Director	YES*	Executive Directors have the same access rights as Agency Administrators; however, they are ranked above Agency Administrators. Agencies must purchase Executive Director licenses from CDSA unless the ED enters data into HMIS or submits reports to CDSA or Federal agencies that require HMIS.
System Operator	N/A	System Operators have access to administrative functions. They can set up new providers/organizations, add new users, reset passwords, and access other system-level options. They can also order and manage user licenses. These users have no access to ClientPoint, or Reports. System Operators help maintain Community Services, but cannot access any Client or service records. CDSA level users only
System Administrator I		System Administrator I users have access to all ***Community Services*** features and functions except the Client/Service Access Information audit report, and System Preferences. System Administrator I users cannot merge Clients and do not have access to the Duplicate Client Report. System Administrator I users can delete Clients that were created by organizations within their organizational tree. System Admin I users can delete needs and services created within the entire organizational tree. Agency Admin has an ART View license. CDSA level users only.
System Administrator II	N/A	System Administrator II users have full and complete access to All ***Community Services*** features and functions. This includes access to Provider Groups and the ability to generate reports for these groups. System Administrators II can delete Clients, needs, and services created across organizational trees. System Administrator II has an ART Ad Hoc license and is responsible for writing all custom reports for the System. CDSA level users only.

Plan for Remote Access: All HMIS Users are prohibited from using a computer that is available to the public or non-Agency employees/volunteers such as family members or clients. Users should not access the System from a public location through an internet connection that is not secured. For example, staff is not allowed to use Internet Cafes, Libraries, Airport Wi-Fi or other non-secure internet connections. The Agency's Privacy Policy must have a plan for remote access if staff will be using HMIS outside of the office such as doing entry from home.

Concerns addressed in this plan should include the privacy surrounding the off-site entry.

- The computer and environment of entry must meet all the standards defined above.
- Downloads to the off-site computer may not include Client identifying information.

User Termination or Extended Leave from Employment: The Agency Administrator should terminate the rights of a user immediately upon suspension or termination from their current position. The Agency Administrator must inform the System Administrator within one (1) day.

If a staff person is to go on leave for a period of longer than 40 days, their password should be inactivated within two (2) business days of the start of their leave. The Agency Administrator must inform the System Administrator within one (1) business day of inactivating a user's license.

The Agency Administrator should review the agency access list and signed agreements on a quarterly basis to ensure that records are up-to-date. The Agency Administrator must provide information about changes to the System Administrator within one (1) business day of the action.

Report Access and Transport: Select HMIS users will have access to agency-level HMIS data in the form of reports and Client case files. Access to this information is based on User Level and is determined based on need. Reasonable care should be taken when reviewing HMIS materials to ensure information is secure.

- Media and documents containing Client-identified data should not be shared outside the HMIS Participating Agencies.
- Printed HMIS information should be stored or disposed of properly.
- All Client records containing identifying information that are stored within the Participating Agency's local computers are the responsibility of the participating agency.
- Media containing HMIS data that is released and/or disposed of by the participating agency should first be processed to destroy any data residing on that media. Degaussing, shredding and overwriting are acceptable methods of destroying data.

Disaster Recovery Plan

The HMIS can be used in response to catastrophic events. The HMIS data is housed in a secure server bank with nightly off-site backup. Data will be immediately available via Internet connection if the catastrophe is in Oregon and can be restored within 24 hours if the catastrophe is where the server bank is located.

HMIS Data System:

- Nightly database backups
- Offsite storage of backups
- 7 day backup history stored locally on instantly accessible RAID storage
- 1 month backup history stored off site
- 24 / 7 access to WellSky's emergency line to provide assistance related to "outages" or "downtime"
- 24 hours backed up locally on instantly-accessible disk storage
-

Agency Emergency Protocol:

- The Agency Administrator will act as the emergency contact liaison between the Agency and CDSA.
- The Agency will include HMIS in their internal emergency response policies including notification the timeline of notification procedures

In the Event of System Failure:

The System Administrator will notify Agency Administrators should a disaster occur at Wellsky Information Systems or in CDSA government offices.

- Notification will include a description of the recovery plan related time lines.
- After business hours, HMIS staff report System Failures to Wellsky using the Emergency Contact protocol.
- The System Administrator will notify Wellsky if additional database services are required.

Data Collection, Types, and Usage

Each participating agency is responsible for ensuring that all Clients are asked a set of questions which answer HUD or local required data elements.

Besides the required elements, the HMIS Administrator will work with the Agency Administrator to identify the most appropriate assessments to complete. In doing so, the HMIS System Administrator will ensure that each program is completing the required data elements as part of their regular Client assessments.

System Changes

Any system change(s), i.e. – new required data elements, merging data elements or programs, etc. must be presented to HMIS Advisory Committee for approval. The System Administrator will determine whether CDSA has the capability to make the changes or contracted out to Wellsky or other third party. CDSA System Administrator will keep record of all requests and changes made. HMIS documents will be updated as needed to reflect the changes.

Agency/Program Reports

Self-Generated: User Agencies can run their own reports using Report Writer or Advance Report Tool (ART). ART requires the purchase of an ART viewer license. Basic Report training for running ART reports is available upon request to CDSA. User Agencies can only run reports using their own Client's data. CDSA is not responsible for the accuracy of any Report Writer reports produced by a User Agency.

CDSA Produced: The Agency Administrator may request a custom program report(s) from the HMIS Analyst by email. CDSA expects requests to be made within a reasonable amount of time of when it is needed.

Victim Service Providers
Victim Service Provider agencies are prohibited from participating in HMIS by the Violence Against Women Act (VAWA).

> **Definition**: Victim Service Provider (VSP)
> A VSP is defined as a private nonprofit organization whose primary mission is to provide services to victims of domestic violence, dating violence, sexual assault, or stalking.
> Providers include rape crisis centers, domestic violence shelter and transitional housing programs, and other programs. A VSP is a designation at the agency level, not the project leve**l** (see 24 CFR 578.3).

Based on funding, VSPs are required to use a comparable database. In this case, those programs are responsible for creating/contracting for this database and are required to ensure that it meets regulations. CDSA will cooperate with these programs to ensure that accurate reporting of aggregated, de-identified data is counted in quarterly and annual reports and tables. Upon request, CDSA will provide VSPs access to a comparable data system.

Inter-Agency & Inter-Departmental Data Sharing

CDSA's HMIS participates in various Oklahoma projects. HMIS data may be exported and used in various data-based projects. If a project requires this data,those Agencies that chose CDSA as their HMIS Lead will be informed of the project request. If approved by the HMIS Advisory Committee, CDSA will then de-identify the HMIS data prior to submission of the project. The purpose of sharing:

- Data visualization for HMIS participating agencies through Tableau
- Data Quality activities
- Research (not client level)
- Program evaluation and design (not client level)

Participating Agency Use of HMIS Data

HMIS Participating Agencies may publish and report using HMIS data collected and entered by their agency. HMIS Participating Agencies may not use data collected and entered into HMIS by other HMIS Participating Agencies without a written agreement between the Agencies.

Release of Data

CDSA will periodically publish public reports about poverty and homelessness in the OK-500 and OK-507 CoC geographic area. No confidential Client data will be included in these reports. The HMIS Analyst will review the reports prior to release.

In order to ensure accurate and consistent interpretation of HMIS data, only CDSA may publish or report using HMIS data. No other CDSA department or division may use HMIS for reporting or publishing activities.

Requests for System Wide Data: Any organization or individual who would like to request system wide poverty and homeless data must complete a Data Request form and submit it to the HMIS Analyst (see supporting documents). The form will include the purpose of the request, type of data needed, time frame, etc. CDSA will attempt to fulfill routine requests in a timely manner. CDSA has the right to accept or reject any request, i.e. – information requested is at a level of detail we can't provide, or data elements that may not be reliable, etc.

If data will be used for publication CDSA should be credited as the source of the data. System Analyst will keep record of requests and the information that was provided.

Data Quality Plan

Data Quality and Completeness

- CDSA will provide training guides, checklists and guidance.
- CDSA will issue proficiency certificates to Users beginning 2025.
- For TH, RRH, PSH project types, Agencies must require documentation at intake of the homeless status of Clients according to the reporting and eligibility guidelines issued by HUD. The order of priority for obtaining evidence of homeless status are (1) third party documentation, (2) worker observations, and (3) certification from the person. Lack of third party documentation may not be used to refuse emergency shelter, street outreach or domestic violence services.
- Data must be entered into HMIS within 24 hours of the event. (see Data Timeliness)
- All staff are required to be trained on the HUD definition of Homelessness, regardless of program type.
- Documentation of HMIS training provided by CDSA and by the participating agency must be available for audit.
- There should be congruity between the following HMIS data elements, based on the applicable homeless definition: (Is Client Homeless, Housing Status, Prior Living Situation and Length of stay at prior living situation are being properly completed).
- If using paper, the intake/exit data collection forms should correctly align with the HMIS work flow. Direct data entry is encouraged.
- The Agency will have a process to ensure that First and Last Names are spelled properly and the DOB is accurate.
    - o An ID may be requested at intake to support proper spelling of the Clients name as well as the recording of the DOB. This is voluntary unless the project requires it for eligibility.
    - o If no ID is available or if the Client chooses not to show ID, staff will request the legal spelling of the person's name.
- The Agency is responsible to determine Clients with significant privacy needs or those who choose not share any data and follow the appropriate policies and procedures to reduce visibility in the HMIS.

- If the System Administrator removes the Client name and other PII from the HMIS at the request of the Agency, the agency must keep a document of the crosswalk of the Client ID and the Client's Name and PII in a secure location on site. This document can be monitored by CDSA and project funders.
- HMIS data must be updated when the Agency becomes aware of a change when possible, or at minimum annually and at exit.
- Agencies have an organized exit process that includes:
  - Clients and staff are educated on the importance of planning and communicating regarding discharge. This is evidenced through staff meeting minutes or other training logs and records.
  - Agency staff are trained in HUD's destination definitions.
  - There is a procedure for communicating exit information to the person responsible for data entry.
- HMIS Analyst regularly runs data quality reports (at least monthly).
- The Administrative Analyst will distribute a quarterly data quality report to all Agency staff and management which provides the percentage of missing or unknown/refused required HUD data elements. The goal is for less than three percent (3%) missing or unknown/refused entries for each data element.

The HMIS data collection years are based on:

1. The operating year of the grant (OY)
2. The fiscal year (FY 07/1 to 06/30)
3. The calendar year (CY 01/01 to 12/31)
4. The federal fiscal year (FFY 10/1 to 9/30)

All data for the data collection years must be complete and accurate no later than the third day of the month following the end date.

Data quality screening and correction activities may also include the following:

- Missing or inaccurate information in Universal Data Element Fields, Program Data fields and local data elements.
- Un-exited Clients using the Length of Stay and Un-exited Client Data Quality Reports.
- Count reports for proper ratio of children to adults in families. (at least 1.25)
- It is recommended that Agencies use HMIS to monitor their performance at least quarterly. CDSA will provide system-wide performance report annually.

Data Timeliness

Data must be entered into HMIS within 24 hours of the event. This includes new client records, project entries, project exits and upon receipt of updated information. Service transactions should also be entered at the time of the service.

The Agency's Agency Administrators are responsible to ensure that data are complete, accurate, and timely. CDSA HMIS Analysts will monitor projects to ensure data completeness and timeliness policies are being followed. A quarterly data quality report will be provided to participating agencies and the HMIS Advisory Committee.

HMIS Use

Each Agency must be logged in and actively using Wellsky Community Services.

- A User Last Login Report will be run every month. This report shows all user activity for agencies in HMIS. All users must be actively engaged in using HMIS.
- All projects will also be subjected to random user audits to ensure that data is being entered and HMIS is being used correctly.
- For any Agency where all User have not logged in within the past month, an informal inquiry e-mail will be sent to the Agency Administrator. The Agency Administrator must write back within 48 hours as to why ***Community Services*** has not been utilized within the report time period.
- All agencies must log in to ***Community Services*** within the last two calendar months (at least one User). If there has not been any user logged in within two calendar months, a more formal disciplinary action will be taken.

Disciplinary Process

The following describes the disciplinary process for not following the agreed upon terms:

- If not logged into HMIS within the last calendar month OR if data is not being entered in a timely manner, an informal inquiry e-mail will be sent. The Agency Administrator must respond within 48 hours.
- If the agency is still not logging into HMIS within the last two calendar months OR if data is still not being entered in a timely manner, an official warning letter will be sent to the Agency Administrator and Executive Director. An official warning letter may also result in a deduction of points for your HMIS score for the CoC competition process.
- If an agency receives two warning letters within the calendar year, this will result in a 0 for the Agencies entire HMIS score for the CoC competition.
- If an agency is still not utilizing the HMIS correctly after two warning letters in a calendar year, a meeting with the appropriate Executive Director (CDSA for OK-500, Kibois for OK-507), Agency Administrator, and applicable CDSA staff will take place to discuss further discipline. This could include loss of federal, state or local funding.

HMIS Monitoring

CDSA is the HMIS Lead for OK-500 and OK-507 and is responsible for monitoring and enforcing compliance by all HMIS Participating Providers with all the HUD requirements and report on compliance to the Continuum of Care and HUD. The Agency Participation agreement explicitly states that each agency will be monitored. Each agency will be monitored at minimum every three years.

Monitoring addresses compliance with the following: national objectives; Client eligibility; project performance; confidentiality and privacy policies; agency agreements with CDSA; overall management systems; financial management and audits; adherence to federal grant regulations; Client records; records maintenance; anti-discrimination, affirmative action and equal employment opportunity.

The objective is to monitor HMIS project recipients to:

- Ensure HMIS Privacy and Security regulations are being met
- Ensure that Client records match HMIS Client records
- Ensure that projects are meeting national data quality objectives
- Ensure that project's and activities recipient's support operates in a consistent, effective and efficient manner, consistent with the project's intent

HMIS Coordinated Entry

An effective coordinated entry process evaluates and connects those most in need in the community with the most appropriate available resources for their situation as swiftly as possible – the process should be low barrier, housing first oriented, person-centered, and inclusive.

In the coordinated entry process, also called Front Door Assessment (FDA), Clients are assessed by a standardized survey at the point of entry and are prioritized accordingly. CDSA uses the HMIS as part of this process. The HMIS is used to:

- Store Assessments
- Run Reports
- Prioritize Client Waitlist
- Maintain the Central Waitlist
- Make Referrals

Grievances

Client Grievances: Clients with a HMIS-related grievance should first identify their concerns to their regular Agency staff member. Upon learning of the grievance, the Agency staff member is required to communicate the concern to their HMIS Agency Administrator for review and possible resolution.

Each participating Agency is responsible for addressing Client questions and complaints regarding the HMIS to the best of their ability and in accordance with their agency grievance policies. Possible actions may include further investigation of incidents, clarification or review of policies, or sanctioning of users (if users are found to have violated standards set forth in HMIS agreements or this Standard Operating Procedures Manual). Participating agencies are also obligated to report all HMIS-related Client grievances to the HMIS System Administrator.

Grievances regarding Coordinated Entry have a separate process.

If a Client grievance is not satisfactorily resolved at the Agency level, the Client may contact the HMIS Administrator who will attempt to resolve the issue. If necessary, the System Administrator will present the problem to the HMIS Advisory Committee (HAC) at their next meeting.

The HAC will be given an opportunity to review the details and facts of a situation and will present recommendations towards resolution to the appropriate CoC Board meeting. The appropriate CoC Board will have final decision-making authority.

Agency Grievances: Any problems related to the operation or policies of HMIS or its participating agencies should be directed to the HMIS Administrator. S/he is responsible for addressing agency–level questions and complaints regarding the HMIS to the best of their ability. Possible actions may include further investigation of incidents, clarification or review of policies, or sanctioning of participating agencies. The HMIS System Administrator is also obligated to report all HMIS-related agency grievances to the HMIS Advisory Committee.

If an agency issue is not satisfactorily resolved by the HMIS System Administrator, the agency may bring the issue to the Data Quality Collaborative. The HMIS Advisory Committee will provide information related to the details and facts of a situation to the HAC as well as recommendations towards resolution. The HAC will have final decision-making authority.

The HMIS System Administrator will be responsible for providing a summary of all grievances and their resolutions to the HAC on a monthly basis.

HMIS Staff Grievances: Any problems with the HMIS Support Staff should first be reported to the HMIS Lead. The HMIS Lead will seek to resolve the issue and will identify staffing concerns to the CDSA Executive Director. Any grievances against the HMIS Lead should be made directly to the CDSA Executive Director for resolution. Grievance forms are located on page x.

Termination of HMIS Participation

Voluntary Termination: To discontinue participation in HMIS, an agency must submit written notice to the HMIS System Administrator. Upon receipt of this written notice, all licenses assigned to that agency will be discontinued within 72 hours.

Involuntary Termination: If the HMIS Advisory Committee decides to terminate an agency from the HMIS, the committee will submit a written notice to the Agency's Executive Director identifying a termination date. On that termination date, all licenses assigned to that agency will be discontinued at 5pm, unless an effective date was otherwise established.

Regardless of the reason for termination of participation in HMIS, any costs associated with transferring/exporting data out of the HMIS will be the responsibility of the terminated agency.

Supporting Documents

CDSA posts the following documents on the CDSA and North Central OK website.
www.cdsaok.org www.ncokcoc.org

- CDSA HMIS Agency Administrator Agreement
- CDSA HMIS Agency Participation Agreement
- CDSA HMIS Data Quality Plan
- CDSA HMIS Data Standards Manual
- CDSA HMIS Policies & Procedures
- CDSA HMIS Privacy Notice
- CDSA HMIS Privacy Script
- CDSA HMIS Privacy Sign
- CDSA HMIS Security Incident Report
- CDSA HMIS Standard Operating Procedures Manual
- CDSA HMIS User Agreement & Code of Ethics

Housing and Urban Development posts the following documents on the HUD Exchange website. https://www.hudexchange.info/resource/3824/hmis-data-dictionary/

- 2024 HMIS Data Dictionary (or most recent version)
- 2024 HMIS Data Standards Manual (or most recent version)
- Data Entry for FY 2024 Data Standards Update (or most recent version)

Revision History

Date	Author	Description