



CDSA HMIS POLICY & PROCEDURES

OK-500 & OK-507

Abstract

HMIS Policy & Procedures approved by HMIS Joint Advisory Committee August 25, 2024
Developed to serve and support rural services providers in Oklahoma
Compiled to ensure HUD HMIS Compliance within OK-500 & OK-507

CDSA HMIS Lead

114 South Independence

Enid, OK 73701

580-242-6131

hmis@cdaok.org

Table of Contents

- Table of Contents 1
- CDSA HMIS Lead History 3
- Common HMIS Acronyms 4
- HMIS Overview 7
- Program Types in HMIS 8
 - HUD Defines 9 Basic Program Types: 8
- Benefits of HMIS 10
 - For People Experiencing Poverty or Homelessness 10
 - For Social Service Providers 10
 - For the Community 10
- HMIS Roles & Responsibilities 11
 - Wellsky Client Services 11
 - Continuum of Care 11
 - The HMIS Lead Agency 11
 - HMIS Joint Advisory Committee (HJAC) 12
 - HMIS System Administrator (System Admin) 12
 - HMIS Information Specialist 13
 - HMIS Agency Administrator 13
 - HMIS Users 14
 - HMIS Participating and Partner Agencies 14
- Policies and Procedures 15
- Privacy and Data Sharing Plan 17
- Client Privacy Policy 19
 - Privacy Policy Definitions 20
- CDSA’s Security Plan 21
 - Wellsky Security Responsibilities 21
 - Access to HMIS 25
- Disaster Recovery Plan 30
 - Data Collection, Types, and Usage 31
- Data Quality Plan 33
 - Data Timeliness 34
 - HMIS Use 34
 - Disciplinary Process 35

HMIS Monitoring	35
HMIS Coordinated Entry	36
Grievances	36
Termination of HMIS Participation	37
Revision History	38
Supporting Documents	39
CDSA HMIS FORMS QUICK LINKS	40
CDSA HMIS DOCUMENTS APPENDIX.....	41
Agency Participation Agreement.....	41
Agency Administrator Agreement.....	41
User Agreement & Code of Ethics	41
Project Set-Up Form	41
HMIS Security Incident Report.....	41
HMIS Grievance Form	41
HMIS Privacy Notice.....	41
Adviso de Privacidad HMIS de CDSA	41
Privacy Script (English)	41
Privacy Script (Spanish)	41
Privacy Sign (English)	41
Privacy Sign (Spanish)	41
Limited Visibility Request (English)	41
Limited Visibility Request (Spanish).....	41
<i>Securing Client Data</i> published by Wellsky, 2019	41

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. 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 increasing their capacity to eliminate homelessness.

Common HMIS Acronyms

ACRONYM &/or TERM	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.
AHAR Annual Homeless Assessment Report	A HUD report to the U.S. Congress that provides nationwide estimates of homelessness, including information about the demographic characteristics of homeless persons, service use patterns, and the capacity to house homeless persons.
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.
CoC Continuum of Care	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.
CHO	Any organization (including its employees, volunteers, affiliates, contractors, and associates)

Covered Homeless Organization	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.
HMIS Homeless Management Information System	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.
HIC Housing Inventory Chart	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.
LOS Length of Stay	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.
LSA Longitudinal Systems Analysis	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 household 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.
PII Personal Protected Information	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.

PIT Point in Time Count	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.
ROI Release of Information	A signed (paper) document or verbally documented disclosure 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 P Stella Performance	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.
SPM System Performance Measures	Seven 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

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

- Makes it possible to maintain intake information over time so the number of times a Client repeats their story to providers is reduced.
- Offers an opportunity to conduct intakes and life histories once; illustrating that service providers consider the Client's time valuable and ensuring Client dignity.
- Makes it possible to coordinate multiple services and streamline referrals. This will help to reduce Client waiting time.

For Social Service Providers

- Provides real-time information about needs and available services for Clients.
- Assures confidentiality by keeping information in a secured system.
- Decreases duplicative Client intakes and assessments.
- Reduces time required to conduct intakes and assessments.
- Tracks Client outcomes and provides a Client history.
- Generates data reports for local use and to meet funding 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.

For the Community

- Helps the community to define and understand the extent of poverty and homelessness throughout North Central Oklahoma
- Provides greater focus for staff and financial resources to the geographical areas, agencies, and programs where services are needed most.
- Allows for better evaluation of the effectiveness of specific interventions, programs, and services.
- Offers local, state, and federal legislators data and information about the population served
- Makes it possible to meet all federal reporting requirements.

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.

The HMIS Lead Agency

- **Community Development Support Association, Inc. (CDSA)**

The HMIS Lead Agency is responsible for:

1. 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.
2. 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 CHOs.
3. Submitting a security plan, data quality plan and privacy policy to the CoC for approval within six months of any changes to the regulations.
4. Reviewing and updating HMIS documents at least annually that incorporates feedback from the HMIS Advisory Committee and CoC approval.
5. 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 (HJAC)

- 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 HJAC 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:

1. Determining guiding principles for HMIS
2. Selecting data elements to be collected in addition to HUD requirements by participating agencies
3. Defining parameters for the release of aggregated HMIS data Evaluating HMIS compliance with HUD data and technical standards
4. Reviewing the HMIS-related performance of the system and of participating agencies
5. Reviewing the adherence to local policies and procedures;
6. Reviewing Security Incident Reports
7. 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:

1. 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
2. Developing training materials
3. Preparing regular trainings for Agency Administrators Authorizing access to the HMIS (Set-Up)
4. Developing Client assessment tools not already included
5. 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:

1. Participating in HMIS readiness assessment
2. Identifying HMIS users and providing or facilitating access to training
3. Granting HMIS access staff members that have received training and demonstrated proficiency in system use and understanding of policies and procedures
4. Monitoring staff compliance with standards of Client consent and confidentiality and system security
5. Enforcing business controls and practices to ensure organizational adherence to policies and procedures including detecting and responding to violations
6. Providing on-site support for the generation of agency reports and managing user licenses.
7. Running reports in Community Services and the Community Services reporting tool for Agency Management and Agency Users
8. Ensuring stability in the agency Internet connection either directly or in communication with a technician
9. 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:

1. Being aware of the confidential nature of data and taking appropriate measures to prevent any unauthorized disclosure of Client information
2. Accurate and timely data entry
3. Complying with all local HMIS policies and procedures Reporting security violations to their HMIS Agency Administrator
4. Users are also responsible for their own actions or any actions undertaken with their usernames and passwords.

HMIS Participating 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:

- 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.
- Client 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:

- The 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 the System 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 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.

Privacy Policy 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 Release of Information (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 of 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's Security Plan

WellSky Security Responsibilities

WellSky's security responsibilities are outlined in the [WellSky Securing Client Data](#) document in the Appendix of this document and 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 are 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 form](#)) 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 Joint 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 Joint 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 Joint 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 Fees for Participating Coordinated Entry Agencies 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.
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. <i>CDSA level users only.</i>
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 and ShelterPoint.

Agency Staff	NO	Agency Staff users have access to ResourcePoint and ShelterPoint. 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, & III	NO	Case Managers have access to all <i>Community Services</i> 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	<p>Agency administrators have access to all <i>Community Services</i> 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.</p> <p>Agency Admins cannot access the following administrative functions: Assessment Administration, Direct Access to Admin>Groups, Picklist Data, Admin>Users>Licenses, or System Preferences.</p> <p>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.</p> <p>An Agency Admin shall not delete or modify a Provider through Provider Admin unless given specific instructions from the System Administrator.</p> <p>Agency Admins have ART View licenses and are responsible for pulling all reports for the Agency</p>
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	N/A	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

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 level (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 Joint 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 are unable to 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 workflow. 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.
 - 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.
 - 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 HMIS 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 Joint 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 recipients 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. 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 in the Appendix of this document.

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.

Revision History

Date	Author	Description
8/26/24	Jade Powell	Recommended for Approval HJAC

Supporting Documents

CDSA posts the following documents and/or forms from the remainder of this document, as well as this document in its entirety, on the CDSA website. www.cdsaok.org

CDSA HMIS follows the Data Standards required by Housing and Urban Development (HUD). Please find additional HUD guidance and information below. CDSA HMIS is aligned to HUD standards, as evidenced in the following documents:

[Current HMIS Data Dictionary](#)

[Current HMIS Data Standards Manual](#)

[CoC Supplemental to Address Unsheltered and Rural Homelessness HMIS Guidance](#)

Additional Information for the Homeless Management Information System (HMIS) is available on the HUD Website at <https://www.hudexchange.info/programs/hmis/>.

CDSA HMIS FORMS QUICK LINKS

[CDSA HMIS Agency Administrator Agreement](#)

[CDSA HMIS Agency Participation Agreement](#)

[CDSA HMIS Local Data Standards Manual](#)

[CDSA HMIS Grievance Form](#)

[CDSA HMIS Policies & Procedures](#)

[CDSA HMIS Privacy Notice](#)

[Aviso de Privacidad HMIS de CDSA](#)

[CDSA HMIS Privacy Script](#)

[CDSA HMIS Privacy Sign \(English & Spanish\)](#)

[CDSA HMIS Project Set-up Form](#)

[CDSA HMIS Security Incident Report](#)

[CDSA HMIS User Agreement & Code of Ethics](#)

[CDSA HMIS Limited Visibility Request Form](#)

[CDSA HMIS User Agreement & Code of Ethics](#)

CDSA HMIS DOCUMENTS APPENDIX

- Agency Participation Agreement..... 1
- Agency Administrator Agreement..... 10
- User Agreement & Code of Ethics..... 15
- Project Set-Up Form..... 24
- HMIS Security Incident Report..... 27
- HMIS Grievance Form..... 29
- HMIS Privacy Notice..... 31
- Adviso de Privacidad HMIS de CDSA..... 34
- Privacy Script (English)..... 37
- Privacy Script (Spanish)..... 38
- Privacy Sign (English)..... 39
- Privacy Sign (Spanish)..... 40
- Limited Visibility Request (English)..... 41
- Limited Visibility Request (Spanish)..... 42
- Securing Client Data published by Wellsky, 2019..... 43



CDSA HMIS FORMS



Continuum of Care Homeless Management Information System Participation Agreement



Which CoC are you a member of? *

Today's Date *

Agency Name *

This agreement entered into on the date specified above between CDSA, Inc., an Oklahoma non-profit corporation (hereafter referred to as "HMIS Lead Agency") and the Agency listed above (hereafter referred to as "HMIS Participating Agency"), outlines points of agreement for the use of the Homeless Management Information System, hereafter known as "HMIS." The HMIS Participating Agency is a Covered Homeless Organization ("CHO") as defined by the U.S. Dept of Housing and Urban Development in Federal Register HMIS Data and Technical Standards Final Notice, dated July 20, 2004 or as amended. As defined by the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the HMIS Participating Agency is:

Is the Agency specified above a "Covered Entity"? *

A Covered Entity. After submission, the Business Associate Agreement will populate to and submission made a part of this HMIS Participation Agreement with all agencies that are Covered Entities as defined by the Health and Insurance Portability Accountability Act of 1996 (HIPAA).

This agreement is effective as of the date shown below and remains in effect indefinitely, unless terminated earlier in writing by either of the parties on 45 days' written notice.

The HMIS is a web-based information management system designed to assist providers of services to homeless and formerly homeless and those at risk of homelessness to facilitate client intake, data collection and reporting, and to determine community resource availability. HMIS also enables the sharing of client information with other providers where allowed by law or authorized by the client to assist in collaboration on client-related activities such as referrals to other agencies, appointment scheduling, coordination of services and case management.

The HMIS utilizes the Community Services (formerly ServicePoint) software product from WellSky. The Community Services (formerly ServicePoint) product is operated from a computing infrastructure operated and maintained by WellSky and administered locally by HMIS Lead Agency and its agents. HMIS Lead Agency may engage an independent contractor, to manage administration on its behalf.

HMIS Participating Agency Responsibilities:

- HMIS Participating Agency will comply with all federal and state laws, rules and regulations that apply to the use of HMIS and the collection, use and disclosure of client information. NOTE: A CHO that is also a Covered Entity under HIPAA/HITECH is not required to comply with the privacy or security standards in the Federal Register HMIS Data and Technical Standards Final Notice, dated July 20, 2004 or as amended if the CHO determines that a substantial portion of its homeless client data is protected health information as defined in the HIPAA rules.
- HMIS Participating Agency will comply with the operational policies and procedures in the Homeless Management Information System Standard Operating Policies and Procedures.

- HMIS Participating Agency will adopt and implement a Privacy Policy that is in compliance with either the Federal Register HMIS privacy and security standards, or the HIPAA rules, as is applicable to HMIS Participating Agency's status as a CHO.
- HMIS Participating Agency will require all HMIS Participating Agency HMIS Users to complete new user training prior to being issued a HMIS User ID.
- HMIS Participating Agency will require all HMIS Participating Agency HMIS users sign the HMIS User Policy Responsibility Statement.
- HMIS Participating Agency will require the HMIS Participating Agency administrator take necessary steps to ensure that user access is discontinued immediately upon the effective date that the HMIS Participating Agency user is no longer employed by the HMIS Participating Agency or otherwise no longer authorized to be user. Action will include, at minimum, notifying the HMIS Lead Agency in writing of user right termination at least five business prior days to effective date or immediately upon termination of rights if prior notice is not available.
- HMIS Participating Agency will verify the accuracy and completeness of HMIS Participating Agency resource information in HMIS on at least an annual basis.
- Cooperate with other agencies utilizing HMIS in the coordination of care and case management for clients accessing services from multiple agencies for the mutual benefit of the client, the agencies, and the community.
- Obtain written authorization from the client using a client authorization for release of protected information form before client information is used or disclosed for any purpose not allowed by the HIPAA rules, Federal Register HMIS privacy and security standards or other applicable laws.
- Retain original signed Authorization for Use or Disclosure of Protected Health Information documentation at least six years from the date they cease to be in effect (from expiration or revocation).
- Safeguard information collected from clients or shared by other organizations per Federal Register the most recent [HMIS Data Standards](#), as amended, and/or HIPAA Privacy rules as applicable.
- Authorize HMIS Lead Agency to create and share de-identified files and reports by using the methods defined in the HIPAA law, for itself and other methods as appropriate and as permitted by the HIPAA Privacy Rule.
- Authorize HMIS Lead Agency to create and share limited data sets as defined and limited by the HIPAA Privacy Rule.

HMIS Lead Agency Responsibilities:

- HMIS Lead Agency will provide the HMIS Participating Agency 24-hour access to the HMIS data collection system, via internet connection.
- HMIS Lead Agency will adhere to the baseline security standards and requirements for system application and hardcopy security as outlined in the Federal Register/vol. 69. No. 146/Friday July 30, 2004 or as amended.
- HMIS Participating Agency retains ownership of the data that it enters into HMIS. HMIS Participating Agency may access this data online via HMIS or can obtain copies of data as extracted files by request from HMIS Lead Agency.
- HMIS Participating Agency retains decision-making authority on items related to HMIS Participating Agency operations and service delivery, including eligibility criteria for services and the means and mechanisms for providing services.
- HMIS Lead Agency will provide model Privacy Notices, Client Release forms, and other templates for agreements that may be adopted or adapted in local implementation of HMIS functions.
- HMIS Lead Agency will provide HMIS Community Services (formerly ServicePoint) administration and user access.
- HMIS Lead Agency will provide both initial training and periodic updates to that training for core HMIS Participating Agency staff regarding the use of HMIS, with the expectation that the HMIS Participating Agency will take responsibility for conveying this information to all HMIS Participating Agency staff using the system.

- HMIS Lead Agency will provide basic user support and technical assistance (i.e., general troubleshooting and assistance with standard report generation). Access to this basic technical assistance will normally be available from 9:00 AM. to 5:00 PM. on Monday through Friday (with the exclusion of holidays). HMIS staff will also be accessible during non-standard operating hours in accord with procedures that will be agreed in writing between HMIS Participating Agency and HMIS Lead Agency.
- HMIS Lead Agency will not publish reports on client data that identify specific agencies or persons, without prior HMIS Participating Agency (and where necessary, client) permission. Public reports otherwise published will be limited to presentation of aggregated data within the HMIS database.
- HMIS Lead Agency's publication practice will be governed by policies established by HMIS Lead Agency and HMIS Participating Agency's designees level for statewide analysis and will include qualifiers such as coverage levels or other issues necessary to clarify the meaning of published findings.
- Update the HMIS Standard Operating Policies and Procedures as needed to meet current requirements and maintain compliance with all federal and state laws, rules and regulations that may apply to the use of the HMIS.
- Notify HMIS Participating Agency in writing at least 30 days prior to the effective date of changes to the HMIS Homeless Management Information Standard Operating Policies and Procedures.
- Execute a HMIS Participation Agreement with all organizations using the HMIS that prohibits the redisclosure of individually identifiable information.
- Act as liaison between HMIS Participating Agency and WellSky Corporation.
- HMIS Lead Agency shall adhere to security standards and requirements for system application outlined in Federal Register/vol. 69 No. 146/Friday July 30, 2004, as subsequently amended.
- Except for claims for which the parties have insurance, and only after any available insurance proceeds are applied to cover the claims, then HMIS Lead Agency shall indemnify, defend and hold harmless HMIS Participating Agency from and against legal liability and damages including any claims, causes of action cost, attorneys' fees or other expenses of any nature arising from any acts, omissions or negligence on the part of HMIS Lead Agency, its' employees, contractors, subcontractors, representatives, agents or designees. To the extent that any such claims, liabilities, costs, damages, or expenses are covered by available insurance purchased by HMIS Lead Agency, HMIS Participating Agency will not be required to reimburse HMIS Lead Agency for the same, or for any deductible amount due to access the insurance coverage. The obligation of HMIS Lead Agency to indemnify HMIS Participating Agency shall not apply to the extent that such application would nullify any existing insurance coverage of HMIS Lead Agency or the portion of any claim of loss in which an insurer is obligated to defend or satisfy the claim. HMIS Participating Agency will remain responsible for its errors or omissions, and those of any HMIS Participating Agency employees, agents, contractors, or commissioners.
- So long as this agreement is in effect, HMIS Lead Agency shall provide HMIS Participating Agency with a certificate of insurance for General Liability with limits of not less than \$1,000,000 per occurrence and \$3,000,000 aggregate. HMIS Lead Agency will also maintain workmen's compensation insurance for all HMIS Lead Agency employees and contractors in the amount required by law. HMIS Lead Agency shall name HMIS Participating Agency as an additional insured on all policies.
- WellSky Corporation is solely responsible for any warranty of the capabilities of the Community Services (formerly ServicePoint) software. In no event shall HMIS Lead Agency be liable for indirect, consequential punitive or special damages. HMIS Lead Agency shall not be responsible for loss of data or interruption of service caused by HMIS Participating Agency or any other person or entity.

Any disputes regarding this agreement shall be resolved under the laws of the State of Oklahoma and any litigation shall be commenced in Garfield County, Oklahoma.

HMIS Participating Agency Name *

First	Last
-------	------

Name, HMIS Lead Agency

Title *

Title

Signature *

×

[draw](#) type

Signature

Date *

Date

A fully executed agreement will be provided to the Agency above by email and mail within 2 weeks of submission. To expedite this process, please email hmis@cdsaok.com after submission

Business Associate Agreement

This Business Associate Agreement ("Agreement") is entered into effective by and between Community Development Support Association (CDSA) Inc. and (the "Covered Entity").

RECITALS

WHEREAS, the Covered Entity and Business Associate have entered into one or more agreements providing, among other things, that Business Associate will perform certain services on behalf of the Covered Entity (collectively, the "Services Agreement"); and

WHEREAS, in order to comply with the Administrative Simplification provisions of the regulations adopted under Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), as set forth in 45 CFR Parts 160, 162 and 164 and as amended by the HITECH Act portion of the American Recovery and Reinvestment Act of 2009, the parties desire to enter into this Agreement in order to comply with such provisions (the "HIPAA Rules") (45 CFR Parts 160 and 164 being referred to herein as the "Privacy Rule");

1. Definitions

Words and phrases used in this Agreement, including but not limited to capitalized words and phrases, which are not otherwise defined herein shall have the meanings assigned thereto in the HIPAA Rules.

2. Obligations and Activities of Business Associate

- a. Business Associate agrees not to use or disclose protected health information other than as permitted or required by this Agreement or as required by law.
- b. Business Associate agrees to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information, to prevent use or disclosure of protected health information other than as provided for by this Agreement.
- c. Business Associate agrees to report promptly to Covered Entity any use or disclosure of protected health information not provided for by this Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR § 164.410 (described in Section 6. below) and any security incident of which it becomes aware.
- d. In accordance with 45 CFR §§ 502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractor of Business Associate that creates, receives, maintains or transmits protected health information on behalf of Business Associate agrees to the same restrictions, conditions and requirements that apply through this Agreement or otherwise to Business Associate with respect to such information.
- e. Business Associate agrees to provide access, at the request of Covered Entity, and in the time and manner reasonably requested by Covered Entity, to protected health information in a designated record set, to Covered Entity in order for Covered Entity to meet the requirements under 45 CFR § 164.524.
- f. To the extent a request is made by the Covered Entity for Business Associate to respond to any request by the Secretary or any other Federal or State authority, Covered Entity shall be responsible for paying for all services related to Business Associate responding to such inquiry and all reasonable costs associated with such response.
- g. Business Associate agrees to document such disclosures of protected health information and information related to such disclosures as would be required for Covered Entity to respond to a request by an individual for an accounting of disclosures of protected health information in accordance with 45 CFR § 164.528.
- h. Business Associate agrees to provide to Covered Entity in a time and manner as may be reasonably requested by Covered Entity, information collected in accordance with Section 2(g) above, to permit Covered Entity to respond to a request by an individual for an accounting of disclosures of protected health information in accordance with 45 CFR § 164.528.

3. Permitted Use and Disclosure by Business Associate

- a. Except as otherwise limited in this Agreement, Business Associate may use or disclose protected health information to perform functions, activities or services for, or on behalf of, Covered Entity as specified in the Services Agreement.
- b. Except as otherwise limited in this Agreement, Business Associate may use protected health information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.
- c. Except as otherwise limited in this Agreement, Business Associate may disclose protected health information for the proper management and administration of the Business Associate, provided that disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

4. Obligations of Covered Entity

- a. Covered Entity will notify Business Associate of any limitation(s) in its notice of privacy practices of Covered Entity in accordance with 45 CFR § 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of protected health information.
- b. Covered Entity will notify Business Associate of any changes in, or revocation of, permission by individual to use or disclose protected health information, to the extent that such changes may affect Business Associate's use or disclosure of protected health information.

- c. Covered Entity will notify Business Associate of any restriction to the use or disclosure of protected health information that Covered Entity has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of protected health information.

5. Permissible Requests by Covered Entity

Covered Entity shall not request Business Associate to use or disclose protected health information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity.

6. HITECH Act

Business Associate agrees to [report to the Covered Entity](#), in writing, within ten (10) business days of the Business Associate's discovery of any "Breach", as such term is defined in the HIPAA Rules. The notification to Covered Entity of a Breach will include: (1) a description of what happened, including the date of the Breach, date of the discovery of the Breach, and affected individuals; (2) a description of the types of unsecured PHI that were involved in the Breach; (3) suggested steps affected individuals should take to protect themselves from potential harm resulting from the Breach; and (4) a brief description of what Business Associate is doing to investigate the Breach, mitigate potential harm, and to protect against future Breaches.

7. Protection of Exchanged Information in Electronic Transactions

If Business Associate conducts any standard transactions for or on behalf of the Covered Entity, Business Associate shall comply, and shall require any subcontractor or agent conducting such standard transactions to comply, with each applicable requirement of 45 CFR Part 162.

8. Term

The term of this Agreement shall be effective as of the Effective Date, and shall terminate when all of the protected health information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy protected health information, protections are extended to such information, in accordance with the provisions of Section 10 below.

9. Termination for Cause

Upon Covered Entity's knowledge of a material breach of this Agreement by Business Associate, Covered Entity shall:

- a. Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement and the Services Agreement if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity; or
- b. Immediately terminate this Agreement and the Services Agreement if Business Associate has breached a material term of this Agreement and cure is not made.

10. Effect of Termination

- a. Except as provided in subsection (b) below, upon termination of this Agreement, for any reason, Business Associate shall return or destroy any protected health information received from Covered Entity or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to protected health information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the protected health information.
- b. If Business Associate determines that returning or destroying the protected health information is infeasible, Business Associate shall subject the protected health information to the same safeguards as for an active engagement. Business Associate shall extend the protections of this Agreement to such protected health information and limit further uses and disclosures of such protected health information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such protected health information.

11. Indemnification

To the extent any damages that may arise under this Agreement are covered by insurance, the parties waive all rights against each other and against the contractors, consultants, agents and employees of the other for damages, except such rights as they may have to the proceeds of such insurance. The parties, as appropriate, shall require of the contractors, consultants, agents and employees of any of them similar waivers in favor of the other parties enumerated herein.

Except as provided above, Business Associate shall be solely responsible for and shall indemnify and hold Covered Entity and its affiliates harmless from any and all claims, fines, penalties, losses, damages, or causes of action (including court costs and the indemnified party's reasonable attorneys' fees) asserted against or suffered by the indemnified party relating to, resulting from, or arising out of any breach of this Agreement by Business Associate, its employees, agents and/or Subcontractors. The indemnified party shall notify Business Associate promptly of any action or claims threatened against or received by the indemnified party and relating to actions or services of Business Associate and/or its agents, employees, and Subcontractors, and shall provide Business Associate with such cooperation, information, and assistance as Business Associate shall reasonably request. Further, Covered Entity shall be solely responsible for and shall indemnify and hold Business Associate and its affiliates harmless from any and all claims, fines, penalties losses, damages or causes of action (including court costs and the indemnified party's reasonable attorneys' fees) asserted against or suffered by the indemnified party relating to, resulting from, or arising out of any claim against Business Associate, its employees, or Subcontractors, related to this Agreement that arises from harm caused by or wrongful or negligent conduct of Covered Entity or its employees or agents. The indemnified party shall notify Covered Entity promptly of any action or claims threatened against or received by the indemnified party and relating to actions or services of Covered Entity or its agents, employees, or Subcontractors, and shall provide Covered Entity with such cooperation, information, and assistance as Covered Entity shall reasonably request. This Section shall survive the termination of this Agreement.

12. Regulatory References

A reference in this Agreement to a section in any statute or in the HIPAA Rules means the section as in effect or as amended.

13. Survival

A Business Associate's obligation to protect the privacy of the protected health information created or received for or from the Plan will be continuous and survive termination, cancellation, expiration or other conclusion of the Agreement.

14. Interpretation and Conflicts

Any ambiguity in this Agreement or the Services Agreement shall be resolved in favor of a meaning that permits the Plan to comply with HIPAA and the HIPAA Rules. In the event of conflicting terms or conditions with prior agreements between the parties, this Agreement shall supersede any such previous agreement.

15. No Third-Party Beneficiary

Nothing express or implied in this Agreement or the Services Agreement is intended to confer, nor shall anything herein confer, upon any person other than the parties and the respective successors or assignees of the parties, any rights, remedies, obligations, or liabilities whatsoever.

16. Governing Law

This Agreement shall be governed by and construed in accordance with the laws of the State of Oklahoma to the extent not preempted by HIPAA, the HIPAA Rules or other applicable Federal law.

17. Notice

All notices, requests, consents, and other communications hereunder will be addressed to the receiving party's address set forth below or to such other address as a party may designate by notice hereunder.

If to the Business Associate:

Community Development Support Association, Inc.

114 S. Independence

Enid, OK 73701

If to Covered Entity, please provide information below: *

IN WITNESS WHEREOF, each of the undersigned has caused this Agreement be duly executed in its name and on its behalf as of the Effective Date.

A fully executed agreement will be provided to the Agency above by email and mail within 2 weeks of submission. To expedite this process, please email hmis@cdsaok.com after submission

Covered Entity *

Business Associate

Community Development Support Association

Name of Authorized Official *

Name of Authorized Official

Authorized Official Title *

Authorized Official Title

Covered Entity Address *

Covered Entity Address

114 S. Independence, Enid, Oklahoma 73701

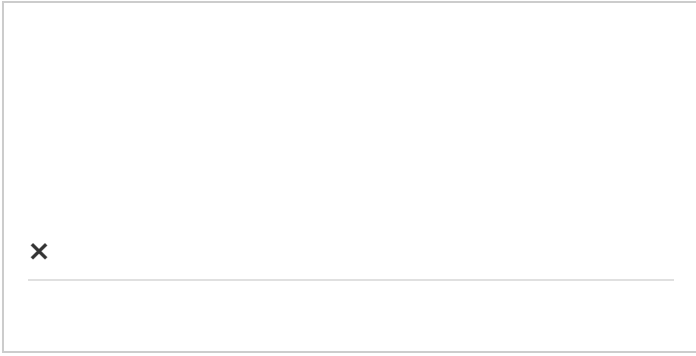
Date of Signature *

Date of Signature

Authorized Official Signature *

Authorized Official Signature



draw type

Submit

Save

CDSA HMIS Agency Admin Agreement



Form instructions: This form must be signed by both the User and the person entered as Executive Director or Direct Supervisor. Please complete as much of the form as you can for your role, then click **Save** at the end of the form. You will also need to fill out the User Agreement Form if you do not already have an HMIS license.

A pop-up window will appear with a link to your incomplete form. You can copy this and send it to the person who needs to complete the other fields or use the **Email me my link** option to email it to them directly.

You will be able to click **Submit** on the form when all required fields (including signatures) are complete. **CDSA HMIS is not notified of your form until it is submitted.** Once a form is opened, you will have 7 days to complete and submit it.

Agency Administrator's Full Name *

Agency Name *

User Position/Role at Agency *

User Email *

User Phone *

Please list all HMIS projects that you will be responsible for:

Click "+Add Item" to add additional projects

Project Name



+ Add Item

About HMIS

The Homeless Management Information System (HMIS) is a web-enabled database used by social service providers within Oklahoma to capture information about the persons they serve.

The fundamental purpose of HMIS is to improve care coordination for persons experiencing poverty and/or homelessness in Oklahoma. HMIS is designed to collect and deliver timely, credible, quality data about services and persons experiencing poverty and/or homelessness. The collected quality information can be used for program improvement and service-planning. Data will be used to complete reporting requirements as established by federal, state and local funders as needed.

HMIS utilizes Community Services (ServicePoint) which is developed, trademarked and copyrighted by WellSky. Community Services (ServicePoint) is a client information system that provides a standardized assessment of consumer need, 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.

The Agency Administrator (Agency Admin) is an Agency staff person who will be the main contact for the Agency and matters regarding the HMIS. The Agency Administrator will be the first contact for user staff for issues concerning the HMIS before the HMIS System Administrator is contacted.

The System Administrator for OK-500 and OK-507 is a CDSA staff person.

I understand and agree to comply with the statement listed above.

Yes

Staff & Training

The Agency Administrator will contact the System Administrator to coordinate training new Users and refresher trainings as needed. The System Administrator will provide New User training and Agency Admin training. Agency Admins are required provide HMIS training to end users (Users) at their agency using materials provided by the System Administrator. The Agency Administrator will inform the System Administrator within one (1) business day if a staff HMIS User leaves the Agency so the System Administrator can de-activate the license upon such notification.

If a User takes a temporary leave of absence (including but not limited to: maternity/paternity leave, medical leave, sabbatical), the Agency Administrator must contact the System Administrator within one (1) days of staff member's departure. Licenses will be temporarily de-activated for staff on a leave of absence, to be re-activated upon return to the Agency. If the leave is extensive (i.e. greater than six (6) months), staff may be subject to a refresher training before the User is able to resume HMIS usage.

I understand and agree to comply with the statement listed above.

Yes

Reports

The Agency Administrator will monitor HMIS data quality by ensuring that Users are entering data in a timely matter and that the assessments contain complete and accurate information. The Agency Administrator and Users will adhere to the requirements of the Data Quality Plan.

The CDSA HMIS Analyst will run a high-level aggregated report monthly to document data completeness and timeliness. The HMIS Analyst will report monthly to the CoC Boards and HMIS Advisory Committee at when meetings are held.

The Agency Administrator will run a data quality report monthly to determine if data is entered completely. The Agency Administrator is responsible to make sure data quality issues are resolved. The Agency Administrator will make sure paper intake (if used) reflects HMIS intake through documentation and record keeping (See: Data Quality Plan). The Agency Administrator is responsible for the following:

1. The Agency Administrator will review data completeness and performance indicators in the ESG-CAPER or CoC-APR on a monthly basis. Specific project types such as PATH or RHY may have additional reports for data quality review.
2. The Agency Administrator will review data on the monthly data quality report card and fix any errors within 10 business days.
3. The Agency Administrator will utilize other report tools, canned reports, ReportWriter, or ART to review Agency's data quality and progress with performance throughout the year.

I understand and agree to comply with the statement listed above.

Yes

Licenses

1. All new User license request must come from the Agency Administrator.
2. The Agency Administrator will be notified if there is a violation of CDSA HMIS Policies & Procedures. The Agency Administrator will be notified in writing if a User license will be revoked or suspended.
3. Inactive licensed User accounts will have their license suspended by the System Administrator after forty days of inactivity. Activity will be monitored by the System Administrator. No notice will be given to the User of the Agency Administrator.
4. A User's license will be de-activated if required training is not completed within the timeframe allowed.
5. When a User's employment with the Agency is terminated, the Agency Administrator will notify the System Administrator immediately so access to the HMIS can be de-activated.

I understand and agree to comply with the statement listed above.

Yes

Additional Responsibilities

1. The Agency Administrator is responsible for updating User profile information. This ensures that CDSA has the most up to date contact information for all Users at your Agency. This needs to be updated any time contact information has changed.
2. The Agency Administrator (or designated Agency HMIS User) will be required to attend bimonthly HMIS Agency Admin meetings.
3. The Agency Administrator is responsible for communication with CDSA staff. This means that emails and phone calls must be returned or answered in a timely manner.
4. The Agency Administrator is responsible to inform System Administrator if there are any Program changes that affect HMIS; i.e. number of beds, sub-population served, new programs, new funding sources, etc.
5. Information received by the Agency at the Agency Administrator meetings or via email from CDSA must be communicated with all Agency Staff.

I understand and agree to comply with the statement listed above.

Yes

Signatures and User Info

An e-copy of this form will be kept on file on the CDSA HMIS CoC Folder. The Agency must also keep a copy of this form on file. Forms for individuals no longer employed by the Agency should be kept on file for seven years following date of termination. System Administrators may, at any time, monitor compliance of this agreement.

Agency Admin Full Name *

Signature *

Today's Date *

×

draw type

Do not SIGN if you are not the person named above

To be completed by Executive Director or Direct Supervisor ONLY:

If you are not the Executive Director or Direct Supervisor, please skip this section. You will send them the form to sign after saving the form.

Executive Director or Direct Supervisor's Full Name *

Executive Director or Direct Supervisor's Email *

Signature *

×

draw type

Today's Date *



Do not SIGN if you are not the person named above

Submit

CDSA HMIS User Agreement & Code of Ethics



Form instructions: This form must be signed by both the User and the person entered as Executive Director or Direct Supervisor. Please complete as much of the form as you can for your role, then click **Save** at the end of the form.

A pop-up window will appear with a link to your incomplete form. You can copy this and send it to the person who needs to complete the other fields or use the **Email me my link** option to email it to them directly.

You will be able to click **Submit** on the form when all required fields (including signatures) are complete. **CDSA is not notified of your form until it is submitted.** Once a form is opened, you will have 7 days to complete and submit it.

User Full Name *

User Email *

User Position/Role at Agency

Is this person collecting data only?

Yes No

Selecting this option will not give you a login. It only permits you to collect data that someone else will enter into HMIS.

User Phone

Agency Name *

Agency Admin responsible for training: *

Agency Admin Email *

A copy of this form will be sent to this Admin's email.

HMIS is a web-based information management system designed to assist providers of services to individuals currently, formerly or at risk of experiencing homelessness to facilitate client intake, data collection and reporting, and to determine community resource availability. HMIS also enables the sharing of client information with other providers when allowed by law or authorized by the client to assist in collaboration on client-related activities such as referrals to other agencies, appointment scheduling, coordination of services and case management. HMIS participating agencies and each User within the system is bound by various restrictions regarding the Client information.

Relevant points about safeguarding client information include:

- It is the client's decision about which information, if any, is to be shared with any Partner Agencies.
- HMIS Authorization for Use and Disclosure of Protected Health Information shall be signed by Client before any identifiable client information is designated in Community Services for sharing with any Partner Agencies. Authorization remains in effect for up to three years unless the client chooses to revoke authorization.
- Client consent may be revoked by the client at any time using the Cancellation for Authorization for Use and Disclosure of Protected Health Information. Client should be given a copy of this document and the original should be retained by the provider.
- User shall insure that prior to obtaining Client's signature, the HMIS Authorization for Use and Disclosure of Protected Health Information (Release of Information) was fully reviewed with Client in a manner to ensure that Client fully understood the information (e.g., securing a translator if necessary).
- The Client shall have a right to receive a copy of any signed Authorization for Use and Disclosure of Protected Health Information.
- Originally signed HMIS Client Authorization for Release of Protected Information documents shall be retained at least six years from the date they cease to be in effect (from expiration or revocation).
- No client may be denied services for failure to provide consent for HMIS data collection.
- Users will comply with all Federal and state laws, rules and regulation that may apply to the use of HMIS and the collection, use and disclosure of client information.

I have read the statement above.

Statement of Confidentiality

Employees, volunteers, and any other persons with access in CDSA HMIS are subject to strict guidelines and requirements regarding the use of the Community Services (ServicePoint) HMIS. The HMIS contains personal and private information on individuals; such information must be treated carefully and professionally by all who access it. Each Client must make an informed decision about which information entered into HMIS may be shared with the other HMIS Partner Agencies. The Client must verbally provide consent to share data after hearing the Privacy Script and/or reading the Privacy Signs posted in the Agency's lobby, client interview room and/or other spaces where Clients may congregate or wait.

I have read the statement above.

User Responsibility

By completing and executing this User Agreement you are requesting a User ID and Password that will give you access to HMIS, and agreeing to comply with the Code of Ethics contained herein. Initial each item below to indicate your understanding and acceptance of the proper use of your User ID and Password. Failure to uphold the ethical and confidentiality standards set forth below is grounds for immediate termination from HMIS.

I have read the statement above.

Note: If you are requesting a collecting data only license, you will not receive a login for HMIS.

User Agreements

Please type your initials under each item indicating that you understand and agree to each. If you do not understand any item, please ask for an explanation and do not initial until you understand and agree.

My User ID and Password are for my use only and must not be shared with anyone. *

I must take all reasonable means to keep my Password physically secure. *

It is my responsibility to keep the HMIS Privacy Sign posted in the lobby and near my work station. *

It is my responsibility to read the HMIS Privacy Script to every head of household each time I collect data for an entry assessment (intake/program enrollment). *

I am required to provide a written copy of the CDSA HMIS Privacy Notice at the request of a Client on the day of the request. *

It is my responsibility to request that the visibility of the Entry Assessments (Entry/Exits) and Service Transaction Needs is modified for 1.) Child Only Heads of Household, 2.) Persons who choose not to share your project data with other HMIS Partner Agencies. *

The only individuals who can view information in the HMIS are the Clients to whom the information pertains, and authorized Users at my organization/program, or at those Partner Agencies with a signed HMIS User Agreement & Code of Ethics forms. *

I may only view, obtain, disclose, or use information necessary to perform my job. *

If I am logged into the HMIS and must leave the work area where the computer is located, I must log-off of the HMIS or lock the computer before leaving the work area. Failure to log off the HMIS or lock the computer appropriately may result in a breach in Client confidentiality and system security. *

I must use the HMIS regularly. Failure to use the HMIS regularly may result in the de-activation or deletion of my license. *

Hard copies of HMIS information must be kept in a secure file. When hard copies of HMIS information are no longer needed, they must be properly destroyed to maintain confidentiality. *

If I notice or suspect a security breach, I must immediately notify my Agency Administrator. In the event it is not possible to contact my Agency Administrator, I must notify the CDSA HMIS System Administrator. *

I can only use the HMIS if I demonstrate competency in HMIS data entry and system use as well as program guidelines. *

I must attend a mandated refresher training one (1) time per year. *

If I take a leave of absence for any reason (maternity/paternity leave, medical leave, etc.) I must notify the CDSA HMIS Administrator immediately so my license can be temporarily de-activated. Upon my return, I may contact the HMIS Administrator to re-activate my account. Contingent upon the length of my leave, I may be subject to attending a refresher training before I can regain access. *

When I terminate employment with this Agency, I must contact the Agency Administrator immediately so my access to the HMIS can be de-activated. *

I will ensure that I am not purposely creating a duplicate client record by checking first and last names, SSN, and DOB before creating a new client and will always using an existing client record if one exists. *

I am responsible for entering accurate and timely (within 24 hours) data on each Client and I am responsible for all data I enter into HMIS. *

I am not to over-write complete data, collected/entered at an earlier time, with incomplete data (i.e. Refused, Don't Know, or Data Not Collected).. *

I am to make every effort to collect complete and accurate information at Intake, Review, Exit, and Follow-up and enter it correctly into the HMIS. *

I am required to update data in any new assessment (Intake, Review, Exit, and Follow-up). *

If I have HMIS System Administrator permission to work remotely, I will maintain the same security/confidentiality standards as when in the workplace. *

AFFIRMATIONS REQUESTED BY OTHER OKLAHOMA HMIS LEAD AGENCIES

Please initial after each statement below.

I have received training on using the HMIS. *

I will accept the Wellsky Community Services (ServicePoint) End User Agreement and agree to be bound by the terms stated in the agreement listed above. *

I will take all reasonable means to keep my password physically secure and private. *

I will not share my login username and password with anyone. *

The only individuals who can view HMIS information are authorized users and the individual client to whom the information pertains. *

I understand I will be held responsible if I allow an unauthorized person to access the system, view client information, make changes to the data or otherwise damage information in the system. *

I will only access HMIS from locations and devices authorized by my agency. *

I will not access HMIS via the web from unauthorized public locations and/or shared devices where the potential exists for viewing client information from unauthorized persons. *

I may only view, obtain, disclose, or use the HMIS information necessary to perform my job. *

I will observe all HMIS user policies regarding safeguarding Client information. *

I will enter accurate, complete information to the best of my ability. *

Hard copy printouts of HMIS individual client data are part of a client's confidential file and must be kept in a secure file. If they are no longer needed, they must be properly destroyed to maintain confidentiality. *

A computer running the HMIS should never be left unattended. If I am logged into HMIS, I must log off before leaving my work area. *

I understand that these rules apply to all users of HMIS, whatever their role or position. *

I agree to maintain strict confidentiality of information obtained through the HMIS. *

I agree that if I allow or notice any breach of confidentiality, I will notify my HMIS Agency Administrator in writing and corrective action will be implemented. *

I understand that failure to comply with all affirmations above will result in immediate and permanent termination of my HMIS license. *

Code of Ethics

A. HMIS Users must treat Partner Agencies with respect, fairness and good faith.

B. Each HMIS User should maintain high standards of professional conduct in the capacity as an HMIS User.

C. The HMIS User's primary responsibility is for his/her Client(s).

D. HMIS Users may not, under any circumstance, train other staff members on the use of HMIS, nor may they share HMIS related information with staff members who do not have any type of Oklahoma HMIS User Agreement & Code of Ethics on file with an Oklahoma HMIS System Administrator.

E. The HMIS User may not make discriminatory comments based on race, color, religion, national origin, ancestry, handicap, age, sex, or sexual orientation in the HMIS.

F. The HMIS User will not use the HMIS with the intent to defraud federal, state, or local government or an individual entity; or to conduct any illegal activity.

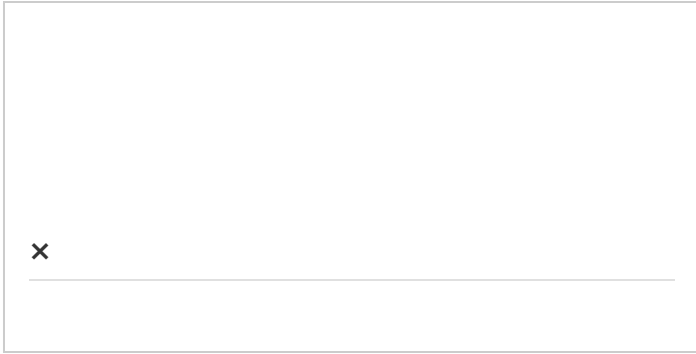
I have read the statement above.

Signatures and User Info

An e-copy of this form will be kept on file at the CDSA. The Agency must also keep a copy of this form on file. Forms for individuals no longer employed by the Agency should be kept on file for seven years following date of termination. System Administrators may, at any time, monitor compliance of this agreement.

User's Full Name *

User Signature *



[draw](#) type

Today's Date *



DO NOT SIGN if you are not the user.

Does this user require access to HMIS on weekends, evenings or nights?

Yes No

This information is used for user monitoring. If this changes, let the system administrator know.

Does this user need an ART license? *

Yes No

ART licenses are used to run additional reports and monitor project data quality. The user will need to schedule an ART training session with CDSA HMIS after account set-up. (Video coming soon!)

User Level (Role) *



When you select a user level, a brief description of the role will appear below.

To be completed by Executive Director or Direct Supervisor ONLY:

If you are not the Executive Director or Direct Supervisor, please skip this section. You can send them the form to sign after saving it.

Executive Director or Direct Supervisor's Full Name *

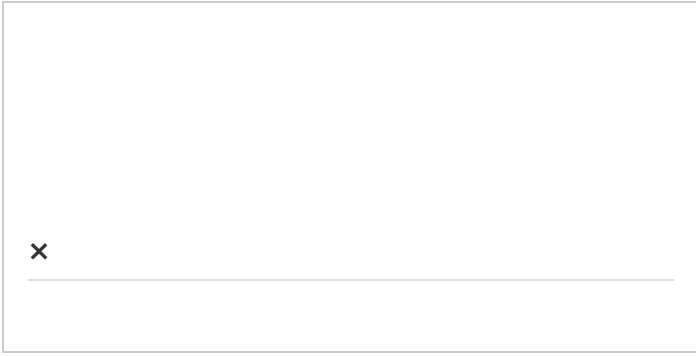


Executive Director or Direct Supervisor's Email *



Executive Director or Direct Supervisor's Signature *

Today's Date *

A large rectangular box for a signature. In the bottom-left corner, there is a small 'x' icon. A horizontal line is drawn across the bottom of the box.A horizontal rectangular input field for a date. A small calendar icon is located in the top-right corner of the field.

draw type

DO NOT SIGN if you are not the person named above.

Submit

Project Set-up Form for CDSA HMIS



Please allow 72 hours for projects to be set up.

Agency Name *

Point Person Name *

Phone *

Email *

Address

Project Details

Name of Project *

Project Start Date *

Address for Public View *

Phone Number for Public View *

Project Description *

Target Population *

DV: Domestic Violence Victims HIV: Persons with HIV/AIDS N/A: Not Applicable

Project Type *

Alternative Shelter ▼

Fund Source Table

	Funding Source *	Grant Identifier	Grant Start Date *	Grant End Date
⊗				

+ Add Item

Services Provided

	Service Type
⊗	

+ Add Item

Additional Project Information

Reporting

If this project has reporting requirements, please upload templates or examples of reports you will be required to complete for this project.

Upload files below

Upload

 or drag files here.

HMIS

HMIS Agency Admin in charge of this project *

First	Last
-------	------

Does this project have special visibility requirements? (limited visibility to certain Agencies or Users)

Yes No

Submit



HMIS Security Incident Report

Data Breach Incident Form



A security incident can involve a data breach is the unauthorized access or acquisition of data that compromises the security, confidentiality, or integrity of data in HMIS. Data may be in any format (electronic, hardcopy or verbal) and may consist of a single piece of data and/or an entire data system.

The participating agency is responsible for immediately mitigating the incident to the extent possible as soon as a possible breach is identified, including notifying clients who may have been impacted by this breach. Data breaches could include but are not limited to:

- HMIS users sharing HMIS account and/or passwords with others.
- Sharing client identifying information with anyone that doesn't have access to HMIS or hasn't been approved to access that data.
- Sharing client identifying information over an unencrypted network.
- Leaving printed documents with client identifying information in an unsecured location.

This form should be used to report any incidents of HMIS data breaches to CDSA HMIS. The form is sent to the HMIS Help Desk automatically when the form is submitted.

Agency Reporting Data Breach *

User Reporting Data Breach *

User Phone Number *

User email *

Describe the data breach that occurred: *

Does the data breach impact all clients in HMIS, or specific clients? *

Estimate the number of client records that are impacted by this data breach: *

What steps has your agency taken to resolve the data breach that occurred? *

Is there any other information that would be helpful for the HMIS team to know to resolve this data breach? *

Submit



HMIS Grievance Form

If you feel a violation of your rights as an HMIS client has occurred or you disagree with a decision made about your "Protected HMIS Information" you may complete this form. Complete this form only after you have exhausted the grievance procedures at the agency you have a grievance with. **It is against the law for any agency to take retaliatory action against you if you file this grievance. You can expect a response within 30 days via the method of your choice.**

Grievances may be submitted to the CDSA HMIS team by either of the following methods:

- Call the HMIS team at (580) 242-6131
- Send this form to:

CDSA
 Attn: HMIS Department
 114 S. Independence
 Enid, OK 73701

Your Name: _____ Date of Grievance: _____

Best Way to Contact You: Phone Mailing Address
 Email Case Manager/Advocate

Your Phone Number: _____ Your Email Address: _____

Your Mailing Address: _____

Case Manager/Advocate Contact Information (optional)

Name: _____ Email Address: _____

Phone Number: _____ Agency: _____

Grievance Information

Name of Individual who violated your privacy rights

Name of Agency who violated your privacy rights

Brief description of grievance (what happened):

What Is HMIS?

The Homeless Management Information System (HMIS) is a web-based information system used by organizations that serve homeless and at-risk individuals in Orange County in order to compile information about the persons they serve.

Why Gather and Maintain Data?

HMIS will gather and maintain unduplicated statistics on a regional level to provide a more accurate picture of our region's homeless and at-risk population. HMIS will also help us understand client needs, help organizations plan appropriate resources for the clients they serve, inform public policy in an attempt to end homelessness, streamline and coordinate services and intake procedures to save client's valuable time, and so much more.

Written Client Consent

Each client must complete a **Consent to Share Protected Personal Information** in order for their identifying information to be shared with other agencies participating in HMIS. If the client refuses to provide consent, only the agency serving the client will have access to his or her information. Clients cannot be denied services for refusing to provide consent. A copy of the form will be provided to the client upon request.

Common Questions

Who can access my information?

Only staff who work directly with clients or who have administrative responsibilities can look at, enter, or edit client information. Please visit our website for a list of the Agencies Contributing Data to HMIS (ochmis.org > About HMIS > Contributing Agencies). Please note that this list can change frequently and without notice; therefore the website should be consulted for the most recent list.

Who will receive my information?

No client identifying information (names, dates of birth, etc.) will be released to entities not participating in HMIS without your consent. Information is stored in an encrypted central database. Only organizations that are contributing data to HMIS and have agreed to abide by the **HMIS Policies and Procedures** will have access to HMIS data.

Don't I have a right to privacy?

Clients do have the right to privacy, and also the right to confidentiality. You are entitled to a copy of the privacy notice upon request. Clients have the right to know who has modified their HMIS record. You also have the right to request access to your HMIS client records, and a printed copy of this data. You have the right to review this data with agency staff. You may not see other clients' records, nor may they see your information.

What if I don't want to provide information?

Clients have the right not to answer any questions, unless entry into a program requires it. You may not be denied services based on your refusal to sign a **Consent to Share Protected Personal Information**.

What if I believe my rights have been violated?

Clients have the right to file a grievance with the agency or with the HMIS Administrative Office at 580-242-6131. Grievances must be filed through written notice. Clients will not be retaliated against for filing a complaint.



CDSA HMIS Privacy Notice



This notice describes the privacy practices of our agency with respect to our use of a database system administered by CDSA, Inc.

Management Information System: We participate in a database system called WellSky Community Services (formerly ServicePoint) that allows community service centers, food pantries, shelters, housing projects, and other social service providers to coordinate services for the people we serve. There is a list of the agencies that participate in the system on www.cdsaok.org. Law enforcement agencies and Oklahoma Department of Human Services do not have access to this system.

Personally Identifiable Information: We collect “Personally Identifiable Information” which identifies you as an individual. This includes your name, date of birth, Social Security Number, or other information that is unique to you. This information is visible in the system to the agencies that use it to coordinate services. If you have a safety concern about other agencies viewing your Personally Identifiable Information, please discuss this with the contact person identified at the end of this document (page 3).

Program Enrollment Information: When you receive services from us, we collect Program Enrollment Information, which may include and information about your race, ethnicity, disabling conditions, previous residence history, income, and other information required by the funders of these services. This information will be visible to other agencies that use the system to coordinate services unless you indicate to us that you do not want your Program Enrollment Information to be visible. It is important to be aware that some projects require information be shared between agencies because they are coordinating services. If a service has a data sharing requirement, then you must share to be eligible for the service. You will be advised of a sharing requirement at the time of project intake.

How We May Use and Disclose Your Information: We may use and disclose your information for the following purposes:

- To provide or coordinate services on behalf of an individual or household
- For functions related to payment or reimbursement for services
- To carry out administrative functions, including but not limited to legal, audit, personnel, oversight and management functions
- For creating de-identified data (where your Personally Identifiable Information has been removed)

Other Uses and Disclosures: We may use or disclose your Information for other reasons, even without your permission. Subject to applicable federal or state law, we are permitted to disclose your Information without your permission for the following purposes:

- Required by Law: We may use/disclose your Personally Identifying Information when such use/disclosure is required by law, subject to the requirements of such law.
- Serious threat to health or safety: We may use and disclose your Personally Identifying Information when necessary to prevent a serious threat to your health and safety or the health

and safety of the public or another person. Any disclosure, however, would only be to someone able to help prevent the threat.

- Abuse, Neglect or Domestic Violence: We may disclose your Personally Identifying Information when the disclosure relates to victims of domestic violence, abuse or neglect, or the neglect or abuse of a child or an adult who physically or mentally incapacitated, where the disclosure is required by law, you agree to such disclosure, or the disclosure is authorized by law and we believe it is necessary to prevent serious harm to you or other potential victims.
- Research: Subject to certain restrictions, we may use or disclose your Personally Identifying Information for approved academic research conducted by an individual or institution that has a formal relationship with us and a written research agreement that requires researchers and data recipients to protect your Personally Identifying Information.
- Law enforcement purposes: Subject to certain restrictions, we may disclose your Personally Identifying Information under certain circumstances if required by law.

Authorization to Use or Disclose Your Personally Identifying Information to a Third Party: Before using or disclosing your Information to a third party (an agency not using the system such as your doctor, a funder of a project you are enrolled in, or another service provider), we will ask for your verbal or written authorization before disclosing your Information. If you choose to agree to disclose your Information, you can later revoke that authorization to stop any future uses and disclosures. However, you cannot revoke your authorization for past uses and disclosures that we have made.

Destruction and De-Identification of Your Personally Identifying Information: We will dispose of or, in the alternative, remove identifiers from, Personally Identifying Information that is not in current use even years after your Personally Identifying Information was created or last changed, unless a statutory, regulatory, contractual, or other requirement mandates we keep it longer.

Request Restrictions: You may request restrictions on uses and disclosures of your Personally Identifying and Program Enrollment Information, unless such restriction is inconsistent with our legal requirements or programmatic and business requirements necessary to operate the program. We are not required to agree to such restrictions, but if we do agree, we must abide by those restrictions.

When you seek services from our Agency, you are verbally informed and/or provided with a brief written Privacy Policy statement called the HMIS Privacy Script. If you choose not to allow your information to be visible to the agencies using the system to coordinate services, then you will be asked to complete a form documenting your decision. This is done to ensure that you were given information about restricted access to some services.

You will still be eligible for most Emergency Services at this Agency or we will refer you to an agency that provides Emergency Services. The ability of this Agency and the network of social service providers using this system to provide supportive services, including housing, may be reduced if you decide to not share information to the other agencies using the system.

- If you are eligible for Supportive Services for Veteran Families (SSVF) projects, you are required to share your Personally Identifying and Program Enrollment Information. Veterans who are homeless and wish to receive housing assistance will need to agree to share information in order to be referred to housing from the Veteran By Name List.
- If you are on the Front Door Coordinated Entry Central Waitlist for Permanent Supportive Housing, Rapid Rehousing, or Transitional Housing, you will need to share your Personally Identifying and Program Enrollment Information in order to be referred to a housing provider.

If you decide to not share your information in the system with the other agencies coordinating services, then you will be asked to provide your all your Personally Identifying and Program Enrollment Information each time you visit an agency that uses this system.

You can request that the restrictions on your Personally Identifying and Program Enrollment Information in the system be changed. You can later agree to share or revoke the visibility of Personally Identifying and Program Enrollment Information to other agencies using the system for any future data entered in to system. However, you cannot restrict visibility for past uses and disclosures that we have made.

Inspect and Obtain Copies: You have the right to inspect and obtain a copy of Personally Identifying and Program Enrollment Information for services we have provided to you. We can also explain to you any information you may not understand.

Amend Information: If you believe that the Personally Identifying Information in your record is incorrect, or if important information is missing, you have the right to request that we correct the existing information or add the missing information. We are not required to remove any information but we may mark information as inaccurate or incomplete and may supplement it with additional information. If you believe there is an error in the system, please discuss this with the contact person identified at the end of this document (page 3)

We reserve the ability to rely on the following reasons for denying an individual inspection or copying of your Personally Identifying Information:

- Information compiled in reasonable anticipation of litigation or comparable proceedings
- Information about another individual
- Information obtained under a promise of confidentiality if disclosure would reveal the source of the information
- The disclosure information which would be reasonably likely to endanger the life or physical safety of any individual

We can reject repeated or harassing requests for access or correction. If we do, we will explain the reason for the denial to you and we will include documentation of the request and the reason for the denial as part of your Personally Identifying Information.

Changes in Privacy Practices: We reserve the right to change our privacy policies and the terms of this Notice at any time and to make the new policies and provisions effective for all Personally Identifying Information, even with respect to the information processed before the amendment.

You have the right to obtain a paper copy of this Notice at any time upon request.

Grievance Process: This agency has a grievance process you can use to address privacy rights you feel were violated. You can request a grievance form from the Agency Contact listed below.

Agency Contact: To make a request, file a concern or complaint, or ask a question please contact the person listed below.

AGENCY NAME: _____		
<input type="text"/>	<input type="text"/>	<input type="text"/>
Agency Contact Name	Contact email address	Contact phone number

Aviso de Privacidad HMIS de CDSA



Este aviso describe las prácticas de privacidad de nuestra agencia con respecto a nuestro uso de un sistema de base de datos administrado por la CDSA.

Sistema de Gestión de Información: CDSA participa en un sistema de base de datos llamado WellSky Community Services (anteriormente llamado ServicePoint) el cual permite que los centros de servicios comunitarios, bancos de alimentos, albergues, proyectos de vivienda y otros proveedores de servicios sociales coordinen servicios para las personas a las que atendemos. Se puede encontrar una lista de las agencias que participan en el sistema en www.cdsaok.org. Las agencias policiales y el Departamento de Servicios Humanos de Oklahoma no tienen acceso a este sistema.

Información de Identificación Personal: Recopilamos "Información de Identificación Personal" la cual lo identifica de manera individual. Esto incluye su nombre, fecha de nacimiento, número de seguro social u otra información que es únicamente acerca de usted. Esta información puede ser vista en el sistema por las agencias que lo utilizan para coordinar servicios. Si usted tiene alguna inquietud de seguridad acerca de qué otras agencias puedan ver su Información de Identificación Personal, hable acerca de esto con la persona de contacto identificada al final de este documento (página 3).

Información de Inscripción en el Programa: Cuando usted recibe nuestros servicios, recopilamos Información de Inscripción en el Programa, la cual puede incluir información acerca de su raza, origen étnico, afecciones que causan incapacidad, historial de residencia anterior, ingresos y otra información requerida por las entidades que otorgan fondos para estos servicios. Esta información podrá ser vista por otras agencias que usan el sistema para coordinar servicios, salvo que usted nos indique que no desea que su Información de Inscripción en el Programa pueda ser vista. Es importante tener en cuenta que algunos proyectos requieren que se comparta información entre las agencias ya que están coordinando servicios. Si un servicio tiene un requisito de compartir datos, entonces usted debe compartirlo para poder ser elegible para el servicio. Se le informará acerca de un requisito de compartir en el momento de admisión al proyecto.

Cómo Podemos Usar y Divulgar Su Información: Podemos usar y divulgar su información para los siguientes propósitos:

- Para ofrecer o coordinar servicios en nombre de un individuo u hogar
- Para funciones relacionadas con el pago o reembolso de servicios
- Para llevar a cabo funciones administrativas, incluyendo, entre otras, funciones legales, de auditoría, de personal, de supervisión y de gestión
- Para crear datos no identificables (donde se ha eliminado su Información de Identificación Personal)

Otros Usos y Divulgaciones: Podemos usar o divulgar su información por otros motivos, incluso sin su permiso. Sujeto a la ley federal o estatal aplicable, se nos permite divulgar su información sin su permiso para los siguientes propósitos:

- Requerido por la ley: Podemos usar / divulgar su Información de Identificación Personal cuando dicho uso / divulgación sea requerido por la ley, sujeto a los requisitos de dicha ley.
- Serias amenazas para la salud o para la seguridad: Podemos usar y divulgar su Información de Identificación Personal cuando sea necesario para evitar una amenaza seria para su salud y seguridad o la salud y seguridad del público u otra persona. Sin embargo, cualquier divulgación solo se haría a alguien con la capacidad de ayudar a prevenir la amenaza.
- Abuso, Negligencia o Violencia Doméstica: Podemos divulgar su Información de Identificación Personal cuando la divulgación se relacione con víctimas de violencia doméstica, abuso o negligencia, o la negligencia o abuso de un niño o un adulto incapacitado física o mentalmente, donde la divulgación es

requerida por ley, usted acepta divulgación, o la divulgación está autorizada por la ley y creemos que es necesario para evitar daños serios a usted u otras posibles víctimas.

- Investigación: Sujeto a ciertas restricciones, podemos usar o divulgar su Información de Identificación Personal para investigaciones académicas aprobadas realizadas por una persona o institución que tenga una relación formal con nosotros y un acuerdo de investigación por escrito que requiera que los investigadores y los destinatarios de los datos protejan su Información de Identificación Personal.
- Propósitos de orden público: Sujeto a ciertas restricciones, podemos divulgar su Información de Identificación Personal bajo ciertas circunstancias si así lo requiere la ley.

Autorización para Usar o Divulgar Su Información de Identificación Personal a un Tercero: Antes de utilizar o divulgar su información a un tercero (una agencia que no utiliza el sistema, tal como su médico, una entidad que otorgue fondos de un proyecto en el que usted se haya inscrito u otro proveedor de servicios), le pediremos su autorización verbal o escrita antes de divulgar su Información. Si elige aceptar divulgar su información, podrá posteriormente revocar esa autorización para detener cualquier futuro uso y divulgación. Sin embargo, no puede revocar su autorización por usos y divulgaciones anteriores que ya hayamos realizado.

Destrucción y Desidentificación de Su Información de Identificación Personal: Eliminaremos o, como alternativa, retiraremos los identificadores de toda Información de Identificación Personal que no esté en uso actual, incluso años después de que su Información de Identificación Personal fue establecida o modificada por última vez, salvo para cumplir con requisitos legales, reglamentarios, contractuales u otros requisitos que nos obligue a mantenerla por más tiempo.

Solicitud de Restricciones: Usted puede solicitar restricciones en los usos y divulgaciones de su Información de Identificación Personal y de Inscripción en el Programa salvo que dicha restricción sea inconsistente con nuestros requisitos legales o requisitos programáticos y empresariales necesarios para operar el programa. No estamos obligados a aceptar tales restricciones, pero si lo hacemos, debemos cumplir con esas restricciones.

Cuando usted procura obtener servicios de parte de nuestra Agencia, se le informa verbalmente y / o se le proporciona una breve declaración por escrito de Política de Privacidad llamada Texto de Privacidad HMIS. También puede encontrar un Letrero de Privacidad en el vestíbulo. Si usted elige no permitir que su información sea vista por las agencias que usan el sistema para coordinar los servicios, se le pedirá que complete un formulario que documente su decisión. Esto se hace para garantizar que se le ofrezca información acerca del acceso restringido de algunos servicios.

Aun calificará para recibir la mayoría de los Servicios de Emergencia en esta Agencia, o le recomendaremos a una agencia que brinde Servicios de Emergencia. La capacidad de esta Agencia, y de la red de proveedores de servicios sociales que utilizan este sistema para facilitar servicios de apoyo, incluyendo vivienda, puede verse reducida si decide no compartir información con las otras agencias que utilizan el sistema.

- Si usted califica para proyectos de Servicio de Apoyo para Familias de Veteranos (SSVF, por sus siglas en inglés), debe compartir su Información de Información de Identificación Personal y de Inscripción en el Programa. Los veteranos que no tienen hogar y desean recibir asistencia de vivienda deberán acordar compartir información para ser referidos a la Lista de Veteranos por Nombre (Veteran By Name List).
- Si usted participa en los programas Front Door Coordinated Entry Central Waitlist for Permanent Supportive Housing, Rapid Rehousing, o bien Transitional Housing, deberá compartir su Información de Identificación Personal y de Inscripción en el Programa para ser recomendado con un proveedor de vivienda.

Si usted decide no compartir su información en el sistema con las otras agencias que coordinan los servicios, se le pedirá que dé toda su Información de Identificación Personal y de Inscripción en el Programa cada vez que visite una agencia que utilice este sistema.

Usted puede solicitar que se modifiquen las restricciones de su Información de Identificación Personal y de Inscripción en el Programa en el sistema. Posteriormente, puede aceptar compartir o revocar la visibilidad de la Información de Identificación Personal y de Inscripción en el Programa a otras agencias que utilicen el sistema

para cualquier información futura ingresada en el sistema. Sin embargo, no puede restringir la visibilidad de usos y divulgaciones anteriores que ya hayamos realizado.

Inspección y Obtención de Copias: Usted tiene derecho a inspeccionar y obtener una copia de la Información de Identificación Personal y de Inscripción en el Programa para los servicios que le hemos ofrecido. También podemos explicarle cualquier información que usted no entienda.

Modificación de Información: Si usted cree que la Información de Identificación Personal en su registro es incorrecta, o si falta información importante, tiene derecho a solicitar que corrijamos la información existente, o bien que agreguemos la información que falta. No estamos obligados a eliminar ninguna información, pero podemos marcar la información como inexacta o incompleta y podemos complementarla con información adicional. Si usted cree que hay un error en el sistema, hable acerca de esto con la persona de contacto identificada al final de este documento (página 3)

Nos reservamos la capacidad de confiar en las siguientes razones para negar una inspección individual o para copiar su Información de Identificación Personal:

- Información compilada en anticipación razonable de litigios u otros procedimientos comparables
- Información acerca de otra persona
- Información obtenida bajo promesa de confidencialidad si la divulgación revelara la fuente de la información
- Información de divulgación que razonablemente podría poner en peligro la vida o la seguridad física de cualquier persona

Podemos rechazar solicitudes de acceso o de corrección que sean repetidas o acosadoras. Si lo hacemos, le explicaremos el motivo de la denegación e incluiremos la documentación de la solicitud y el motivo de la denegación como parte de su Información de Identificación Personal.

Cambios en las Prácticas de Privacidad: Nos reservamos el derecho de cambiar nuestras políticas de privacidad y los términos de este Aviso en cualquier momento, y hacer que las nuevas políticas y disposiciones sean efectivas para toda Información de Identificación Personal, incluyendo con respecto a la información procesada antes de la modificación.

Usted tiene derecho a obtener una copia impresa del presente Aviso en cualquier momento si usted así lo solicita.

Proceso de Reparación de Agravio: Esta agencia cuenta con un proceso de reparación de agravio que usted puede usar para abordar los derechos de privacidad que usted considera que han sido infringidos. Puede solicitar un formulario de reparación de agravio de parte del Contacto de la Agencia que se encuentra a continuación.

Contacto de la Agencia: Para hacer una solicitud, presentar una inquietud o queja, o para hacer una pregunta, comuníquese con la persona que figura a continuación.

NOMBRE DE AGENCIA: _____		
<input type="text"/>	<input type="text"/>	<input type="text"/>
Nombre de Contacto de la Agencia	Dirección de correo electrónico de contacto	Número de teléfono de contacto



About Your Information

In order to best assist you, we use a database to manage our services. Your information is visible to a limited number of Oklahoma social service providers and protected using the highest standards. Law enforcement and DHS have no access to this system. Allowing your information to be viewed allows us to better serve you. You'll have improved access to services such as basic needs, employment and housing. This information will help us understand community needs and is used to advocate for funding. If you have any questions or would like a copy of the Privacy Notice, let me know.

Are you ready to get started?



Acerca de su Información

Para poder ayudarlo mejor, utilizamos una base de datos para administrar nuestros servicios. Su información puede ser vista por un número limitado de proveedores de servicios sociales de Oklahoma y está protegida con las más altas normas de seguridad. La policía y el DHS (Departamento de Seguridad Nacional) no tienen acceso a este sistema. Al permitir que su información sea vista, nos permite servirle mejor. Usted tendrá un mejor acceso a los servicios, tales como de necesidades básicas, de empleo y de vivienda. Esta información nos ayudará a comprender las necesidades de la comunidad, y también se utiliza para abogar para obtener fondos. Si tiene alguna pregunta o si desea una copia del Aviso de Privacidad, dígame.

¿Está bien si comenzamos ya?

This Agency Uses



Community Services



- In order to better assist our clients, we store personal information we collect about people we serve in a computer database system.
- The information collected in the system is protected using the highest standards and in compliance with all applicable laws, and is only visible to a limited number of social service agencies with whom we collaborate.
- The information we collect helps us run programs, improve services, secure funding, and better understand your needs. Some of the information we collect may be required by organizations that fund the operation of this program. We only collect information that is needed or required.
- We assume that, by requesting services from our agency, you agree to allow your information to be viewed by the other agencies using the system.
- We will talk to you about this system when we ask you for your information, and you will have an opportunity to ask questions.
- **If you have a safety concern, you may not want your information to be visible to the other agencies in the system. If this is the case, please discuss this with a staff member.**

THIS IS NOT A COMPLETE STATEMENT OF YOUR INFORMATION RIGHTS. For a complete statement of your information rights, please ask a staff person for a copy of our Privacy Notice. If you have any questions about our computerized record-keeping system and how it might affect you, feel free to talk about your concerns with a staff member.

Esta Agencia Utiliza



Community Services



- Con el fin de prestar mejor asistencia a nuestros clientes, almacenamos la información personal que recopilamos sobre las personas que atendemos en una base de datos digital.
- La información recopilada en el sistema está protegida por medio de las más altas normas de seguridad, y de conformidad con todas las leyes aplicables, y solo puede ser vista por un número limitado de agencias de servicios sociales con las que colaboramos.
- La información que recopilamos nos ayuda a implementar programas, mejorar servicios, asegurar fondos y a comprender mejor sus necesidades. Parte de la información que recopilamos puede ser un requisito de parte de las organizaciones que facilitan los fondos para la operación de este programa. Solo recopilamos información que es necesaria o requerida.
- Suponemos que, al solicitar servicios de nuestra agencia, usted acepta permitir que su información sea vista por las otras agencias que utilizan el sistema.
- Hablaremos con usted acerca de este sistema cuando le solicitemos su información, y usted tendrá la oportunidad de hacer preguntas.
- Si tiene inquietudes de seguridad, es posible que no desee que su información sea vista por las otras agencias del sistema. Si este es el caso, hable acerca de esto con un miembro del personal.

LA PRESENTE NO ES UNA DECLARACIÓN COMPLETA DE SUS DERECHOS DE INFORMACIÓN. Para obtener una declaración completa de sus derechos de información, solicite a un miembro del personal una copia de nuestro Aviso de Privacidad. Si tiene alguna pregunta acerca de nuestro sistema computarizado de mantenimiento de registros y cómo podría afectarlo, no dude en hablar acerca de sus inquietudes con un miembro del personal.



Limited Visibility Request

Client Name _____ Date of Birth _____
Head of Household
 Project/Provider Name in WellSky _____ Provider ID _____
 Date of Enrollment Intake Assessment _____ Agency Name _____

I do not want my information that I provided to this agency to be shared with other agencies using the computer database system called WellSky Community Services (formerly called ServicePoint).

I understand that this request may reduce my access to some services, including housing.

I understand that Veterans eligible for Supportive Services for Veteran Families (SSVF) projects are required to share Personally Identifying and Program Enrollment Information.

I understand that I can change my decision to share my information at any time. Information already shared cannot be taken back or revoked.

I do not want this **Program Enrollment Information** to be shared.

- to all other Agencies; or
- to a specific Agency: _____
Agency Name

List all dependents in the household that are included in this request.

Name	Age	Name	Age

Sign

_____ Client (Head of Household) Signature	_____ Date
_____ Printed Name of Intake Worker/Agency Staff	<input type="checkbox"/> Yes <input type="checkbox"/> No
_____ Signature of Intake Worker/Agency Staff	_____ Privacy Script read/provided?
	_____ Date

Staff Notes to Agency Administrator

Is there a safety issue for this client? Yes No

Explain:

Instructions: Submit with Entry/Exit Intake Assessments to HMIS Agency Admin

