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 if the Privacy Script which is read or shown to every household.

Revocation of Consent

If a Client chooses to revoke the Consent to Share, it should be understood that only data going forward will not be shared. Historical data will remain shared.

Use of Anonymous Client Feature

This feature is not used in CDSA HMIS as it is not reportable.

CDSA'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.