# 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.<br>**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 responseto 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.<br>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.<br>*CDSA level users only.* |
| Volunteer | NO | Volunteers have access to ResourcePoint. These users can also view basic demographic information about Clients on the Profile screen, but they are restricted from viewing other assessments. A volunteer can create new Client records, make referrals, or check Clients in and out of shelters. Administrators often assign this user level to individuals who complete Client intakes and refer Clients to agency staff or a case manager. In order to perform these tasks, volunteers have access to some areas of ClientPoint 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 ***Community Services*** features except those needed to run audit reports and features found under the Admin tab. They have access to all screens within ClientPoint, including assessments and service records. Case Manager II users can also create/edit Client infractions if given access by an Agency Administrator or above. Case Manager III users have the added ability to see data down their provider's tree like an Agency Admin. |
| Agency Administrator | NO | Agency administrators have access to all ***Community Services*** features, including agency level administrative functions. These users can remove users from their organization, as well as edit their organization's data. They also have full reporting access with the exception of two reports: Duplicate Client Report and the LSA Export.<br>Agency Admins cannot access the following administrative functions: Assessment Administration, Direct Access to Admin>Groups, Picklist Data, Admin>Users>Licenses, or System Preferences.<br>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.<br>An Agency Admin shall not delete or modify a Provider through Provider Admin unless given specific instructions from the System Administrator.<br>Agency Admins have ART View licenses and are responsible for pulling all reports for the Agency |
| Executive Director | YES | Executive Directors have the same access rights as Agency Administrators; however, they are ranked above Agency Administrators. Agencies must |

| | | |
|---|---|---|
| | | purchase Executive Director licenses from CDSA unless the ED enters data into HMIS or submits reports to CDSA or Federal agencies that require HMIS. |
| System Operator | N/A | System Operators have access to administrative functions. They can set up new providers/organizations, add new users, reset passwords, and access other system-level options. They can also order and manage user licenses. These users have no access to ClientPoint, or Reports. System Operators help maintain Community Services, but cannot access any Client or service records. CDSA level users only. |
| System Administrator | 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.<br>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.<br>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.<br>System Administrators II can delete Clients, needs, and services created across organizational trees.<br>System Administrator II has an ART Ad Hoc license and is responsible for writing all custom reports for the System.<br>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.