Homeless Management Information Systems

Policy & Procedures Manual

Updated December 7, 2021

I. HMIS Roles & Responsibilities Defined

1. Continuum of Care

HMIS Advisory Committee

The HMIS Advisory Committee is responsible for approving all system-wide policies and procedures that will be implemented within the Akron/Summit County HMIS.

Membership of the Advisory Committee will be established according to the following guidelines:

1. There will be a concerted effort to find replacement representatives when participation has been inactive or inconsistent from the organizations involved in the project;
2. There will be a proactive effort to fill gaps in the membership of the Committee in terms of constituency representation: consumer representatives, shelters for both families and individuals, other homeless services organizations, and government agencies that fund homeless assistance services.

The role of the Committee is to provide consumer (provider, homeless consumers, and community stakeholders) input on an ongoing basis to the HMIS project. However, the delegates to the Committee have final decision-making authority on the selected key issues that follow. These issues include:

1. Determining the guiding principles that should underlie the implementation activities of the HMIS project and participating organizations and service programs;
2. Selecting the minimal data elements to be collected by all programs participating in the HMIS project;
3. Defining criteria, standards, and parameters for the release of aggregate data;
4. Ensuring adequate privacy protection provisions in project implementation.

2. United Way of Summit County (UWSM) HMIS Administrator & Technical System Administrator staff

HMIS Administrator
HMIS Level of Access: System Administrator II
The United Way of Summit County (UWSM) HMIS Administrator is the primary contact between the Akron/Summit County Continuum of Care, the HMIS Advisory Committee, and the HMIS Site Administrators.

HMIS Coordinator
HMIS Level of Access: System Administrator II.
The HMIS Trainer will be responsible for developing training curriculum, coordinating training calendars with Site Administrators, and running ongoing training classes for all Service Point end users. HMIS training may be administered by the HMIS Administrator.

Technical Support
UWSM will provide technical support by phone and/or computer shadowing between the hours of 8:00am to 4:00 pm, Monday through Friday. Any system emergencies outside of those hours will be supported by a telephone voicemail system. A message left on our support phone line outside of normal working hours and on weekends will be addressed within the next working day. Requests can also be submitted to HMIShelpdesk@uwsummit.org for response within 48 hours.

The goal of the UWSM HMIS Administrator is to respond to Connecting Agency needs within one business day of the first contact.

The support hotline and help desk e-mail will be staffed by the HMIS Administrator and the HMIS Coordinator. Level of HMIS Access may vary depending on who provides support.

3. **Agency Administrator**

HMIS Site Administrator
HMIS Level of Access: Agency Administrator
Each Connecting Agency will designate an HMIS Site Administrator and send that person's name and contact information to the UWSM HMIS Administrator. Changes to that information should be promptly reported. The HMIS Site Administrator must have an individual e-mail address. The HMIS Site Administrator is the primary HMIS contact at the agency. This person will be responsible for:

1. All activity associated with the agency including oversight of all agency staff who generate or have access to client-level data stored in the system software to ensure adherence to the operating procedures outlined in this document.
2. Will be held responsible for enforcing established policy for any misuse of the software system by his/her designated staff.

3. Providing a single point of communication between the end users and the UWSM Technical staff around HMIS issues.
4. Ensuring the stability of the agency connection to the Internet and ServicePoint, either directly or in communication with other technical professionals;
5. Organizing initial and ongoing Training for their agency users.
6. Ensuring that access to the system be granted to authorized staff members only after they have received training and satisfactorily demonstrated proficiency in use of the software and understanding of the Policies and Procedures and agency policies referred to above.
7. Providing site support for the generation of agency reports.
8. Managing agency user licenses; and
9. Monitoring compliance with standards of client confidentiality and ethical data collection, entry, cleansing and retrieval.
10. Allowing access to the software system based upon need. Need exists only for those shelter staff, volunteers, or designed personnel who work directly with (or supervise staff who work directly with) clients or have data entry responsibilities.
11. Enforcing business controls and practices to ensure organizational adherence to the HMIS Policies and Procedures. This includes detecting and responding to violations of the Policies and Procedures or agency procedures.
12. Notifying all users in their agency of interruptions in service.
13. Ensure data entry commences in the live system within thirty (30) days after receiving the appropriate training(s).
14. Ensure that all data entry is completed in the live system for each program within two (2) days.

Designating one primary HMIS contact and “power-user” at each agency increases the effectiveness of communication both between and within agencies. Each Connecting Agency should choose its HMIS Site Administrator.

4. **Agency Staff and Volunteers**

Agency Users
HMIS Level of Access: May vary by user responsibility.
Connecting Agencies are responsible for communicating needs and questions regarding the HMIS directly to their HMIS Site Administrator. If the Site Administrator is unable to resolve the issue, the Site Administrator will contact the UWSM HMIS Administrator via e-mail or phone.

Resource Specialist III Level:	Access is limited to ResourcePoint module. This role allows the user to search the database of area agencies and programs and view the detail screens for each agency or program. Access to client or service records is not given. This person can update their own agency and program information. This access level can also edit the system-wide news.
Volunteer Level:	Access to ResourcePoint module is limited, access to ClientPoint, and limited access to service records. A volunteer can view or edit basic demographic information about clients (the profile screen), but is restricted from viewing detailed assessments. A volunteer can enter new client records, make referrals, or check-in/out a client from a shelter. Normally, this access level allows a volunteer to complete the intake and then refer the client to agency staff or a case manager.
Agency Staff Level:	Agency staff has access to ResourcePoint, limited access to ClientPoint, full access to service records and access to most functions in Service Point. However, Agency Staff can only access basic demographic data on clients (the profile screen). All other screens are restricted, including assessments and case plan records. They have full access to service records. Agency Staff can also add news items to the newswire feature. There is no reporting access.
Case Manager Level:	Has access to all features excluding administrative functions. They have access to all screens within ClientPoint, including the assessments and full access to service records. There is full reporting access for all record open to them in ServicePoint.
Agency Administrator Level:	Agency Administrators have access to all features including agency level administrative functions. This level can add/remove users for his/her agency and edit their agency and program data. There is full reporting access for all record open to them in ServicePoint. They cannot access the following administrative functions: Assessment administration, Picklist Data, Licenses, Shadow Mode, or System Preferences
Executive Director Level:	Same access rights as Agency Administrator but ranked above Agency Administrator.
System Administrator I Level:	Same access rights to client information (full access) as Agency Administrator. However, this user has full access to administrative functions except Shadow Mode and System Preferences.
System Administrator II Level:	Full and complete access to the system. Can perform Shadow Mode for technical support.

f. Any agency that is found to have consistently and/or flagrantly violated security protocols may have their access privileges suspended or revoked.

g. All individual user sanctions are imposed by the Executive Director of the Participating Agency. If an Agency is found to be in violation, the sanction will be imposed by the HMIS Advisory Committee.

h. Any user found to be in violation of security protocols will be sanctioned accordingly. Sanctions may include but are not limited to; a formal letter of reprimand, suspension of system privileges, revocation of system privileges, termination of employment and criminal prosecution.

III. Agency Readiness Assessment and Training

Participating Agencies must complete the following Agency readiness assessment procedure and training before they will receive a Password and Logon to the live HMIS.

1. **Identify Agency HMIS Administrator:** The Agency Executive Director/President of the participating agency should select an individual as the designated Agency HMIS Administrator. The designated employee will complete an HMIS Site Administrator Agreement form. Agency Participation Agreements should be signed and turned in to the HMIS Administrator at UWSM.

2. **Identify Staff Participants**: The Agency Executive Director/President and Agency HMIS Administrator will identify all agency staff that will have access to the HMIS and the level of access needed for each user. Each User will complete a User Participation Agreement and turn it in to the HMIS Administrator at UWSM. All participating agency staff must complete all user participation forms.

3. **Evaluate Agency Hardware**: The HMIS Administrator will meet with the Agency HMIS Administrator to evaluate if each user has the appropriate hardware and Internet connection (Internet connection greater than 56K/ 90v). Participating agencies must at least provide the Internet connection.
   In the event that hardware must be provided to an Agency, the agency agrees to maintain the integrity of the initial setup provided by UWSM. If the agency terminates participation in the HMIS project, all hardware provided will be returned to UWSM. Consulting time spent to reconfigure software setup to access HMIS will be charged to the agency at the current UWSM consulting rate.

4. **Evaluate Assessment and Report Customization needs**: The HMIS Administrator will meet with the Agency HMIS Administrator to review the Agency's main intake form and data collection needs. It will be the decision of each agency if additional Assessments are needed to collect additional data needed for reporting. Standard Data Elements and APR required data will be available as standard Assessments and reports. Additional customized reporting needs may be postponed if they are not critical for the Agency to go live on the system.

5. **Evaluate Training Needs for Staff**: The HMIS Administrator will meet with the Agency HMIS Administrator to determine the training needs of each individual staff person. (All users should be familiar with Windows and basic mouse skills before attending basic HMIS Data Entry training.)

6. **Logon and Date Entry Training**: The HMIS Administrator will set up training dates with the Agency HMIS Administrator for all staff training. All staff training will take place in a Training version of the HMIS. No live data will be entered in the Training database. A temporary training logon and password will be assigned to each user. This training will take place in the UWSM computer lab or at the agency whenever necessary. The HMIS Administrator and Agency Administrator will also discuss any agency specific policies and custom processes with agency staff at this time.

7. **Standard Report Training:** The HMIS Administrator will set up Agency Report training for all staff that will have access to this feature. The main focus will be on how to create standard HUD required reports. If additional customized agency reporting is needed, this will be postponed until the agency is proficient with required data entry and reporting.

8. **Practice Entry Online**: Once Data Entry and Report training is complete, the agency will practice entering additional fake data into the training database from their Agency location. The HMIS Administrator will evaluate additional training needs at this time based on issues that arise.

9. **Interview Protocols**: Participating agency completes the development of client interview protocols with consultation from the HMIS Advisory Committee. Protocols for completing client consents are tested within the agency.

10. **Assess staff readiness and Agency HMIS Administrator readiness:** The HMIS Administrator will schedule a final meeting and training evaluation for all staff as needed. If the Agency Administrator and HMIS Administrator agree that the agency staff are ready, user ID's and Passwords will be created by the HMIS Administrator and given to each agency user. The Agency Administrator will manage password maintenance at the agency from that point forward. Any change in user status at the agency should be reported by phone or email to the HMIS Administrator the same day. Agency Data entry begins.

11. Reassessment and Monitoring:The HMIS Administrator will run ongoing training to address any agency staff turnover issues, or additional training and support that may be needed.

It is the responsibility of the Agency Administrator to communicate to the HMIS Administrator when additional agency training is needed.

All initial training and user creation in HMIS should be done by the HMIS Administrator. Performance will be tracked by the Agency Administrator and evaluated with the HMIS Administrator for areas to improve the process if needed. Once live data entry at the agency has been fully (90%) integrated into the agency's daily operation for at least 2 months, participating organizations can begin using the information for internal evaluation and reporting requirements.

III. Technical Support and Other Support

1. **System Availability**
   The intent of UWSM is that the HMIS database server will be available 20 hours a day, 7 days a week, 52 weeks a year to incoming connections. Nightly backups of the HMIS data will run between 12:00am and 4:00am. In the event of planned server downtime, the UWSM Systems Manager will inform agencies as much in advance as possible in order to allow Connecting Agencies to plan their access patterns accordingly.

   In the event that the database server is or will be unavailable due to disaster or routine maintenance, the UWSM HMIS Administrator will contact the Agency Site Administrators and inform them of the cause and duration of the interruption in service.

2. **HMIS related support**
   Connecting Agencies will provide their own Computer Hardware and Internet connections and technical support related to maintenance of those connections. In the event that UWSM, provides computer hardware, the agency is still responsible for maintaining their own Internet connection. UWSM will provide support on hardware provided to the agency as long as the agency maintains the integrity of the initial setup of the hardware and software provided by UWSM. Many of the hardware systems that are provided for this project are refurbished and donated and cannot handle additional software downloads. Any additional software will need to be approved/installed by UWSM where the hardware has been provided by UWSM.
   The HMIS technical support staff does not support hardware or software problems that are the result of unrelated/unapproved software downloads that may interfere with the integrity of the initial hardware setup. Additional consultant fees will be charged to the agency to correct these connection issues.

3. **UWSM Technical support (when, response time)**
   UWSM will provide technical support by phone and/or online computer shadowing between the hours of 8:00am to 4:00 pm, Monday through Friday. Any system emergencies outside of those hours will be supported by a telephone voicemail system. A message left on our support phone line outside of normal working hours and on weekends will be addressed within the next working day.
   The goal of the UWSM HMIS Administrator is to respond to Connecting Agency needs within one business day of the first contact. Each onsite Agency Administrator should act as the first level of contact before calling the HMIS Administrator. If the onsite Agency Administrator cannot resolve the problem, then the Agency Administrator should contact the HMIS Administrator by phone or email.

4. **Grievances**
   Agency Grievances
   Any problems related to the operation or policies of the Akron/Summit County HMIS should be directed to UWSM through the HMIS Administrator. If the issue at hand is unable to be resolved at that level, the Agency may bring the issue to the HMIS Advisory Committee.

   The HMIS Advisory Committee has final decision-making power over all aspects of the Akron/Summit County HMIS. In order for the Akron/Summit County HMIS to serve as an adequate tool for Connecting Agencies and as a guide for system-wide planning, any HMIS problems must be addressed by UWSM and the HMIS Advisory Committee to effect system-wide change.

   Through the Agency Site Administrator, Connecting Agencies will bring HMIS problems to the attention of UWSM through the HMIS Administrator. If UWSM cannot resolve the problem, the UWSM HMIS Administrator will present the problem to the HMIS Advisory Committee. The HMIS Advisory Committee shall have the final say in all matters regarding the Akron/Summit County HMIS.

   Client Grievances
   The UWSM HMIS staff will be available to discuss and resolve agency HMIS problems.

   If a problem is not satisfactorily resolved by UWSM, the HMIS Administrator will present the problem to the HMIS Advisory Committee. Clients will contact the Connecting Agency with which they have a grievance for resolution of HMIS problems. Connecting Agencies will report all HMIS related client grievances to the UWSM HMIS Administrator. All grievances will be documented and made available to the HMIS Advisory Committee.

Each Connecting Agency is responsible for answering questions and complaints from their own clients regarding the Akron/Summit County HMIS. UWSM will monitor the overall use of the HMIS and will respond if users or Connecting Agencies fail to follow the terms of the HMIS agency agreements, breach client confidentiality, or misuse client data.

Connecting Agencies are obligated to report all HMIS-related client problems and complaints to the UWSM HMIS Administrator, who will document and present all complaints to the HMIS Advisory Committee to determine the need for further action.

These actions might include further investigation of incidents, clarification or review of policies, or sanctioning of users and agencies if users or agencies are found to have violated standards set forth in HMIS Agency Agreements or the Policies and Procedures Manual.

V. Cost, Equipment, Participation Requirements

1. **Internet Connectivity:** Connection to the internet is the sole responsibility of the participating agency and is a requirement to participate in the Akron/Summit County HMIS.

2. **Information Security Protocols:** The following security licenses/protocols are integrated into the project and are paid for by the current HUD grant for each planned participating agency within the 3-year project implementation.

Required ServicePoint Licenses*
(3-year commitment, early withdrawal charges are an additional cost)
WellSky ServicePoint License
WellSky Support
WellSky Security Software License
WellSky Security Support

Optional Microsoft Office, File Storage, Back-Ups on UWSM's Network*
Microsoft Office
Network space, Technical support, etc.

* Once all HUD funded licenses have been used, additional license requests will be at the cost of the agency. Cost is $600 per computer per year. A 3-year commitment is required to maintain this pricing. Early withdrawal will result in a pro-rated surcharge of $500 per computer for the first year. Costs may increase or decrease over time due to vendor product price changes. If an agency is planning on submitting a grant to cover additional license requests, please contact UWSM for current pricing information.

3. **Maintenance of onsite computer equipment:** Computer equipment provided by UWSM will be supported by the HMIS technical staff as long as the integrity of the initial setup is maintained by the agency. Computer equipment owned by each agency will be maintained and supported by the participating staff within their own agency. HMIS technical staff will provide the initial setup to access the UWSM Citrix mainframe.

   Minimum Computer requirements:

   a. PC with a 2 Gigahertz or higher processor, 40GB hard drive, 512 MB RAM,
   b. Operating system: Microsoft Windows 7, 8 or higher
   c. Most recent version of Google Chrome, Safari or Firefox.
   d. A broadband Internet connection or LAN connection.
   e. Virus protection updates

4. **Identification of a Site Administrator to serve as primary contact:** Each participating agency will be required to complete a form that is signed by the Agency Director which designates an onsite full-time staff person as the Agency Administrator. A description of the Agency Administrator responsibilities is listed in this manual under the section defining Project Roles and Responsibilities.

5. **Additional user license requests**
   The Agency Administrator should obtain a User License Request Form using the HMIS HelpDesk email address: **hmishelpdesk@uwsummit.org**

   The form will be completed by the Agency Administrator, the User, and the Agency Director. The form should include a description of the users' job functions which create the need for the requested level of access to the HMIS.
   The form will be forwarded to the UWSM HMIS Administrator, who will create the user license with a temporary password. This information will be transmitted by email to the Agency Administrator. The Agency Administrator will give the information to the user. The first time the user logs onto the HMIS, a password change will be requested so the Agency Administrator will not know the user's password.

   NOTE: Any additional licenses requested after the initial agency set up will be available on a first come first serve basis while HUD prepaid licenses are available, after that licenses will be available to that agency for a charge per additional user. Contact the UWSM HMIS Administrator for price information. All new users MUST complete training and assessments before they can receive an HMIS ID and Password.

6. **Customization Requests (Assessments, Reports, etc.)**

   All onsite Agency Administrators have the access ability to customize the agency profile, reset passwords and customize reports. In the event an additional assessment is needed in order to collect client data, a written request should be sent by email from the Agency Administrator to the HMIS Administrator detailing the customization and the date needed. Customized assessments past initial agency setup will have second priority to new agency setup in the Akron/Summit County HMIS Implementation.

VI. Inter-Agency Data Sharing, Client Consent, and Access to Core Database

1. **Inter-Agency Data Sharing:**

   a. Personally Identifiable Information entered into the Akron/Summit County HMIS by participating agencies will only be accessible to CoC participating agencies.
   b. All participating agency profiles will be initiated with an Open Security status within the ServicePoint software.
   c. Agency Administrators at both participating agencies who wish to share client information must complete an Inter-Agency Data sharing release and have a completed client consent form to be eligible to share client information within the Akron/Summit County HMIS.
   d. Participating agencies will specify the data sections that will be shared with the other identified agencies who wish to share the same client data.
   e. Participating agencies who wish to share client data must contact the HMIS Administrator, schedule additional training, and complete all required consent forms before a change will be made to the client's online profile within HMIS.

2. **Client Consent:**

   a. All participating agencies will post a Client Notice at the point of data collection with the agency to inform clients of their intent to collect and enter data into the Akron/Summit County HMIS. Participating Agency staff will thoroughly explain the client notice to each client. Client consent to collect information and maintain confidentiality within that agency in an open status will be assumed.
   b. All participating agency profiles will be initiated with an Open Security status within the ServicePoint software.
   c. Client information will only be shared between participating agencies if a client consent form has been signed and participating agencies have completed all processes required in the Akron/Summit County policies and procedures regarding inter-agency data sharing.
   d. The client has the right to revoke consent in writing at any time. Written revocation must be submitted to the Agency Administrator. The Agency Administrator will then work with the HMIS Administrator to close the client profile. Any data that has already been shared will not be able to be closed.

VII. Quality and Confidentiality Control of Data

1. **Data Integrity:** Akron/Summit County HMIS Users will be responsible for the accuracy of their data entry. In order to test the integrity of the data contained in the HMIS, the Systems Administrator will perform regular data integrity checks on the HMIS. Any patterns of error will be reported to the Agency Administrator. When patterns of error have been discovered, users will be required to correct data entry techniques and will be monitored for compliance.

2. **Data Integrity Expectations:** Participating agencies will provide the following levels of accuracy and timeliness:
   a. All names will be accurate;
   b. All required data fields will not exceed 5% null response per month;
   c. All services provided will be compatible with the providing program;
   d. In all reports of shelter provided for a client, the client must be eligible to receive shelter services from the listed provider; and
   e. Data entry for all entry/exit records, Universal Data Elements (UDEs), Program Specific Data Elements (PSDEs), and services provided must be entered into HMIS 2 days from the date of intake whenever it is not reliant on another agency's intake process (i.e. an AMHA issued voucher).

3. **HMIS Administrator and Agency Administrator:** The System Administrator will perform regular data integrity checks on the HMIS. Any patterns of error at a Participating Agency will be reported to the Agency Administrator. When patterns of error have been discovered, users will be required to correct data entry techniques and will be monitored for compliance.

4. **Participating Agencies:**
   Participating Agency approved staff will have access to retrieve any individual and aggregate data entered by their own programs. Participating Agencies will not have access to retrieve individual records entered by other programs except when data is explicitly shared through the HMIS Agency Agreement, and with the explicit consent of the client.

5. **Public:**
   a. The HMIS Administrator, on behalf of the HMIS Advisory Committee, will address all requests for data from entities other than Participating Agencies or clients. No individual client will be provided to any group or individual that is neither the Participating Agency, which entered the data, nor the client without proper authorization or consent.
   b. All requests for data from anyone other than a Participating Agency or client will be direct to the HMIS Administrator at UWSM and will be approved by the HMIS Advisory Committee. As part of the HMIS Administrator's regular employment functions, periodic public reports about homelessness and housing issues in Akron/Summit County Ohio will be issued. No individually identifiable client data will be reported in any of these reports.

6. **Data Retrieval Support:**
   a. Participating agencies will create and run agency-level reports.
   b. The Agency Administrator will be trained in reporting by the HMIS Administrator. The HMIS Administrator will be a resource for report creation.

VIII. Limitation of Liability and Ownership of Agency Data

It is the intent of UWSM, City of Akron, Summit County, the City of Cuyahoga Falls, and the City of Barberton that each participating agency within the Akron/Summit County HMIS be the owner of the all client data collected and stored by the HMIS for each agency.

All data is protected and secure by the policies, technology, and security protocols in place within the HMIS database server.

All participating agencies take full responsibility of ownership and confidentiality protection of any and all data that is collected at their agency and/or downloaded from the HMIS.

IX. Data and User Access

Data Assessment and Access

Access to all central server computing, data communications and sensitive data resources will be controlled. Access is controlled through user identification and authentication. Users are responsible and accountable for work done under their personal identifiers. Access control violations must be monitored, reported and resolved. UWSM staff will work to ensure that all sites receive the security benefits of the system while complying with all stated policies.

Access to Core Database

1. No one will have direct access to the Akron/Summit County HMIS database through any means other than the ServicePoint software, unless explicitly given permission by the HMIS Administrator during a process of software upgrade or conversion.
2. UWSM will monitor access of the HMIS database server and employ security methods to prevent unauthorized database access.
3. Access to client data will be tightly controlled using security technology and restrictive access policies. Only individuals authorized to view or edit individual client data will have access to that data.

Physical Security and Location

The Summit County HMIS data center is located at WellSky Systems in Shreveport, Louisiana. 24-hour security is provided. During normal business hours, separate, limited key access is required to access the server room. In addition, key access is required for entry into the main office building after normal business hours.

Firewall Protection

To further enhance security, firewalls are in place on all servers we host. As detailed below, there are multiple levels of firewall security:

1. The *ServicePoint* application and database servers are separate from the WellSky Systems internal network.
2. WellSky Systems utilizes an industry standard Intrusion Detection System to pinpoint unauthorized attempts at accessing our network and to shield your data in the event of such an attempt.
3. Only regular and secured HTTP traffic are permitted through to the WellSky application servers.
4. Only regular and secured HTTP reply traffic is allowed from the WellSky application servers.
5. Outgoing access to the web is prohibited.
6. As a security policy, specifics on the type of equipment, protocols, and procedures in use are never revealed.

SSL Data Encryption
WellSky Systems utilizes industry Standard, 128-bit SSL encryption to encrypt client data as it travels "over the wire" from our data center to the user's desktop. SSL encryption is a required security item and is implemented on all live web application servers.

Database Encryption
WellSky Systems also offers the robust, ActiveCrypt software application to provide database encryption for *ServicePoint*. This optional level of security encrypts key elements of data that can be tied to individual customer clients and provides a balance between security and the overall application performance.

User Authentication
ServicePoint™ can 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, ServicePoint™ automatically shuts them out of that session.

Application Security
In addition to restricting access to only authorized users, ServicePoint™ utilizes a system of multiple access levels. These levels automatically detect the user access level and controls access to appropriate data.

Database Security
Wherever possible, all database access is controlled at the operating system, through installation of a PKI certificate, and database connection level for additional security.

Media and Hardcopy Protection
Partner Agencies must establish procedures to handle client paper records. Issues to be addressed include the following: identifying which staff has access to the client paper records and for what purposes, allowing staff access only to those records of clients with whom they work with or for data entry purposes, how and where client paper records are stored, length of storage and disposal procedure, and the disclosure of information contained in client paper records.

Printed versions of confidential data will not be copied or left unattended and open to unauthorized access. Media containing client-identified data will not be shared with any agency other than the owner of the data for any reason. HMIS information in hardcopy format will be disposed of properly by shredding finely enough to ensure that information is unrecoverable.

System Administrator Access
Access to all of computing, data communications and sensitive data resources will be controlled. Access is controlled through user identification and authentication. System Administrators are responsible and accountable for work done under their personal identifiers. Access control violations must be monitored, reported and resolved. UWSM staff will work to ensure that all sites receive the security benefits of the system while complying with all stated policies.

System Access Monitoring
HMIS automatically tracks and records access to every client record by use, date, and time of access. HMIS project staff at UWSM will monitor access to system software. HMIS Administrator staff will regularly review user access privileges and remove identification codes and passwords from their systems when users no longer require access. HMIS Agency Administrators are required to provide immediate communication to the HMIS Administrator at UWSM when an employee no longer requires access.

Administration and System-wide Data
Agency Administrators will have full access to their own HMIS agency profiles and user profiles. Agency Administrators can edit users, maintain updates to agency profiles, and reset user passwords.

Data Security
Wherever possible, all database access is controlled at the operating system, through installation of a PKI certificate and database connection level for additional security. Only the IT System Administrator will have access to changing information in the database at the server level. When this is done an appropriate written summary of the information changed will be logged by the HMIS Administrator.

Unnamed/Anonymous Clients
If an agency feels that entry of client's names into HMIS presents an imminent threat to their safety (mostly Domestic Violence clients), the agency may elect to enter all client data as unnamed clients. When entering unnamed clients, it is incumbent upon the agency to keep a record of the client's unique anonymous ID to avoid duplication of entry.

When the Unnamed Client feature is used, HMIS generates a client ID number for the client record that the agency maintains in a secure location along with the person's name. The only way to access the client record is to use the client ID number.

The following is a list of required actions an agency must do when using the anonymous client feature:

1. Enter the client's gender and date of birth. This ensures that aggregate reports detail the correct number of males vs. females and adults vs. children served.

2. Keep a record of this client's anonymous ID on file and be sure to give your anonymous client the unique ID assigned to him or her. The unique ID is found in the Last name field on the Profile screen. You will need the unique ID to retrieve the client record.

Creating unnamed records will still allow unduplicated counts in reports, but will limit an agency to enter all clients as either unnamed or named and therefore this option should only be used if absolutely necessary.

X. Agency Termination of Participation

Participation in the Akron/Summit County HMIS is mandatory for ESG and CoC funding recipients. For agencies receiving HUD funding, not participating in HMIS will jeopardize future HUD funding.

To discontinue participation, the agency must submit written notice to the HMIS Administrator at UWSM. Upon receipt of this written notice all licenses assigned to that agency will be discontinued and closed immediately.

The agency will incur any costs involved associated with transferring/exporting data out of the Akron/Summit County HMIS at their request.

All Agency User Agreements regarding client confidentiality related to any information that has been downloaded from the HMIS prior to the Agency Termination of Participation will remain in effect indefinitely.

***Special Note:** Any additional licenses or service contracts that have been purchased by the agency outside of the HUD provided services may incur an early withdrawal fee. Please see HMIS Policies relating to Costs of Additional Licenses.

XI. License Commitment and Usage Policy within HMIS

Once an agency agrees to participate within the HMIS and accepts use of a ServicePoint user license, the Agency is required to adhere to the following participation requirements:

1. All users must complete HMIS training and an HMIS User Agreement form to be granted live system access.
2. Once a ServicePoint user license is activated on the live system, the Agency is required to begin entering live data into the HMIS as part of their normal intake process within a 15-day period.
3. If an Agency is inactive with client entry for more than 30 days, the ServicePoint user license will be deactivated and the Agency must provide intent of continued participation to the HMIS Administrator. If changes have occurred within the HMIS within those 30 days, the Agency may be required to attend additional user training before their license will be re-activated.
4. Agencies inactive for more than 90 days may lose rights to their user license and access to HMIS. Reactivation of an inactive license is subject to availability of licenses and HUD funds available at that time and may require the Agency to pay license fees on their own in order to reactivate the license. Reactivation will include attending HMIS training again.
5. No more than 1 user can be assigned to a ServicePoint license at one time.
6. Current data entry for ESG funded agencies is required, as stated in their ESG Contracts with the City of Akron. HMIS reports will be provided to the City of Akron on a monthly basis and agencies who are not current in their data entry may jeopardize timely payments from the City of Akron.

XII. Security Plan

Background

The Department of Housing and Urban Development (HUD), with the Interim Rule, requires implementation of security standards. Security standards are directed to ensure the confidentiality, integrity, and availability of all HMIS information; protect against any reasonably anticipated threats or hazards to security; and ensure compliance by end users. Written policies and procedures must comply with all applicable Federal law and regulations, and applicable state or local governmental requirements.

1. All administrative, physical, and technical safeguards shall be implemented within 6 months of initial approval of this security plan.
2. If one or more of these standards cannot be implemented, UWSM shall justify the implementation delay and produce a plan of action.

Administrative Safeguards
The administrative actions, policies, and procedures required to manage the selection, development, implementation, and maintenance of security measures to protect HMIS information.

Security Officer: UWSM and each Contributing HMIS Organization (CHO) must designate an HMIS security officer to be responsible for ensuring compliance with applicable security standards. For UWSM, this person shall be the HMIS Administrator.

Workforce Security: Each CHO shall conduct background checks on the HMIS security officer and on all administrative users and submit the reports to UWSM. Unless otherwise required by HUD, background checks may be conducted only once for all HMIS users.

Security awareness training and follow-up: UWSM shall ensure that all users receive security training prior to being given access to the HMIS, and that the training curriculum reflects the policies of the CoC and the requirements of this part. HMIS security training is required annually.

Reporting security incidents: CHOs will report any security breaches to client data immediately to UWSM so appropriate notification protocols can be determined, executed and follow up preventative action may be carried out. UWSM will notify CHOs of all security breaches, regardless of whether if happens at the server (Administrator) or the client (CHO) level and provide a corrective action plan to meet any HUD-determined predefined threshold when reporting is mandatory, as established by HUD in notice.

Disaster recovery plan: We will use WellSky Systems, LLC disaster recovery plan, with regard to electronic data as it is housed in their physical location, which includes protocols for communication with staff, the CoC, and CHOs and other requirements established by HUD in notice.

Annual security review: UWSM shall complete an annual security review to ensure the implementation of the security requirements for itself and CHOs. This security review shall include completion of a security checklist ensuring that each of the security standards is implemented in accordance with the HMIS security plan.

Contracts and other arrangements: UWSM shall retain copies of all contracts and agreements executed as part of the administration and management of the HMIS or those necessary to comply with the policies outlined in the HMIS security standards.

Please refer to WellSky Securing Client Data in reference to HMIS Client Information Security.

Physical Safeguards

Access to areas containing equipment, data, and software will be secured. All client-identifying information will be strictly safeguarded in accordance with the latest technology available. All data will be securely protected to the maximum extent possible. Ongoing security assessments to include penetration testing will be conducted on a regular basis.
Scope:

1. Server hardware physical security (Locked office)
2. Server software security (Location Access Controls and Username accounts)
3. Network software security (Firewall protection)
4. Network hardware physical security (Locked office)
5. Wire security (SSL Encryption)
6. Client data security (Protegrity Encryption)

UWSM shall annually review and revise all physical measures, policies and procedures to protect the HMIS.

Technical Safeguards

1. Anti-virus protection shall be installed on each workstation which is used to access the HMIS, whether accessed from the CHO or remotely from another location. This anti-virus shall be updated automatically and said workstations shall be scanned for viruses at least weekly
2. All computing resources which will be used to access the HMIS will satisfy the following measures:
    - Will be protected at all times by a firewall
    - User access through the internet will be controlled at all times through the use of PKI
    - Participating agency or a user access may be suspended or revoked for suspected or actual violation of the security protocols.
3. All potential violations of any security protocols will be investigated
4. Any user found to be in violation of security protocols will be sanctioned accordingly. Sanctions may include but are not limited to; a formal letter of reprimand, suspension of system privileges, revocation of system privileges, termination of employment and criminal prosecution
5. Any agency that is found to have consistently and/or flagrantly violated security protocols may have their access privileges suspended or revoked
6. The HMIS Advisory Committee imposes all sanctions and reports to Funders.
7. All sanctions can be appealed to the CoC Executive Committee.

UWSM shall annually review and revise policies and agreements that protect and control access to electronic HMIS information.

XIII. Data Quality and Monitoring Plan

UWSM, in its efforts to meet the regulations as outlined in the HEARTH Act of 2009, has created the following Data Quality & Monitoring policies to present to the HMIS Advisory Committee. This plan is meant to be a starting point, subject to future revisions as needed, while incorporating the key elements identified in the HUD Toolkit for Developing a CoC Data Quality Plan (October 2009). These elements include; Timeliness, Completeness, Accuracy, Monitoring, and Incentives/Enforcement. The plan below describes how HMIS of Akron/Summit County will implement a data quality and monitoring plan. Excerpts from the current policies and procedures document are also included.

Data Quality Plan

Timeliness

1. Current applicable policy: Data entry for all entry/exit records, Universal Data Elements (UDEs), Program Specific Data Elements (PSDEs), and services provided must be entered into HMIS 2 days from the date of intake whenever it is not reliant on another agency's intake process.
2. Purpose: to ensure data is accessible for agency, community level, and federal reporting in as close to real time as possible and to improve data accuracy for community policy and needs decision-making purposes. Reducing the time period between data collection and data entry will increase the accuracy and completeness of client data.
3. Proposed Standard (may vary by program type):
   Data entry for all entry/exit records, Universal Data Elements (UDEs), Program Specific Data Elements (PSDEs) as outlined in the 2020 HMIS Data and technical Standards or required by the CoC, and services provided must be entered into HMIS 2 days from the date of intake whenever it is not reliant on another agency's intake process. For programs participating in central intake, information should be updated/entered within two days from program entry, program exit, and any certification/recertification required by HUD, the CoC, or other Funder. Included data elements that will be monitored are:
   a. Universal data elements (All)
   b. Program specific data elements (2020 Data Standards & CoC)
   c. Entry/Exits (All)
   d. Services (All)
   e. ROIs (All)
   f. Funder-required updates to assessment information (disabilities, income, non-cash benefits, residence, etc.) will continue to be required on the already established funder-required schedule.

Completeness

1. Current applicable policy: Information entered into the Akron/Summit County must meet the following levels of completeness and accuracy:
   a. All names will be accurate;
   b. All required data fields will not exceed 5% null response per month;
   c. All services provided will be compatible with the providing program;
   d. In all reports of shelter provided for a client, the client must be eligible to receive shelter services from the listed provider.
2. Purpose: To ensure that HMIS of Akron/Summit County can accurately describe the clients and services provided to clients who are accessing services. A complete record also is important for reporting for the use of data in any community level reporting as well as for HUD required processes such as NOFA and AHAR/LSA which can affect funding for the CoC and its providers.
3. Proposed Standard:

Information entered into the Akron/Summit County must meet the following levels of completeness and accuracy:

1. All names will be accurate;
2. All required data fields will not exceed 2% null response;
3. All "Client Doesn't Know" or "Client Refused" responses will not exceed 5%;
4. All services provided will be compatible with the providing program;
5. In all reports of shelter provided for a client, the client must be eligible to receive shelter services from the listed provider.
6. Bed Utilization rates: Emergency Shelters, Transitional Housing, and Permanent Supportive Housing programs and CoC Coordinators will review utilization rates quarterly using data in HMIS.
   a. HMIS staff will send quarterly utilization reports to CoC Coordinators to review and pass on to programs. This process can help determine whether data is being completely entered. Low utilization or utilization over 100% can be a sign that data is not being entered or exited correctly. In can also indicate changes in programs, such as bed counts, that must be accurately counted.

Accuracy/Consistency

1. Current applicable policy: Akron/Summit County HMIS Users will be responsible for the accuracy of their data entry. When patterns of error have been discovered, users will be required to correct data entry techniques and will be monitored for compliance.

2. Purpose: To ensure that data in HMIS is collected and entered in a common and consistent manner.
3. Proposed Standard:
   Accuracy/Consistency of data collected and entered into HMIS will be maintained through the following:
   a. The HMIS Lead will create, update and provide HMIS end users with training materials and reports that will guide data entry in a clear and concise manner.
   b. The HMIS lead will provide HMIS users with feedback when necessary in an effort to help agencies reach the desired goals of the CoC and the HMIS Advisory Committee.
   c. Akron/Summit County HMIS Users will be responsible for the accuracy of their data entry. Data entered in HMIS will clearly match data documented in the client file. Updates to client data entered in HMIS must also be clearly documented in the client file. When patterns of error have been discovered and feedback has been provided, users will be required to correct data entry techniques and will be monitored for compliance.

Data Quality Process/Monitoring

1. Current applicable policy: The HMIS Lead is responsible for "Monitoring compliance with standards of client confidentiality and ethical data collection, entry, cleansing and retrieval".
2. Purpose: To ensure that the standards for timeliness, completeness, and accuracy are met and that data quality issues are identified and resolved.
3. Proposed Standard:

All participants in CoC/HMIS initiatives are responsible for monitoring compliance with standards of client confidentiality and ethical data collection, entry, cleansing and retrieval through the following roles:

1. The HMIS Lead will provide monthly data completeness reports, annual HMIS agency audits and other means deemed necessary by the CoC and the HMIS Advisory Committee, HMIS staff will monitor and assist providers in correcting data and updating program information as needed.
2. The CoC Lead will support the HMIS lead in reviewing the reports, agency audits, and request that program providers make any necessary changes to their data.
3. Program providers will review their data, audit results, and make necessary corrections to meet the above data standards.
4. Agencies and HMIS End Users provide timely updates to CoC HMIS staff regarding any changes to programs

Incentives/Enforcement

1. Current applicable policy: None
2. Purpose: To hold the entire community accountable for meeting the needs of those we serve, HUD and other entities through high quality data collection methods and policies.
3. Proposed Standard:
   The CoC Lead will award additional points on the annual CoC application to the HMIS Lead and participating agencies for full compliance of the Policies & Procedures, the Data Quality and Monitoring Plan, and other benchmarks/goals implemented by the CoC and the HMIS Advisory Committee. Failure to do so will result in a lower ranking on the CoC annual application which could lead to complete or total defunding of a program.

XIV. Definitions and Terminology

Audit Trail: A record showing who has accessed a computer system and what operations he or she has performed during a given period of time. Most database management systems include an audit trail component.

Authentication: The process by which users validate their identity.

Confidentiality: (Told in confidence; imparted in secret; of or showing trust in another; confiding) A client's right to privacy of the personal information that was communicated in confidence to a case manager (or other agency staff) that is stored within the HMIS.

Confidential Data: (Information that identifies clients contained within the database). Examples include social security number, name, address, or any other information that can be leveraged to identify a client.

Emergency Shelter: Any facility whose primary purpose is to provide temporary shelter for the homeless in general or for specific populations of the homeless.

Encryption: Conversion of plain text into unreadable data by scrambling it using a 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.

Encryption Solutions: Secure Socket Layer (SSL): A communications protocol used to secure all sensitive data. SSL is normally described as wrapping and encrypted envelope around message transmissions over the Internet.

Database: A computer database is a structured collection of records or data that is stored in a computer system. A database relies upon software to organize the storage of data. In other words, the software models the database structure in what are known as database models (or data models). The model in most common use today is the relational model. Other models such as the hierarchical model and the network model use a more explicit representation of relationships

Firewall: A hardware and/ or software system that enforces access control policy between two networks.

Informed Consent: A client is informed of options of participating in an HMIS system and then specifically asked to consent. The individual needs to be of age and in possession of all of his faculties (for example, not mentally ill), and his/her judgment not impaired at the time of consenting (by sleep, illness, intoxication, alcohol, drugs or other health problems, etc.).

Internal Data: Information scheduled, but not yet approved, for publication. Examples include draft reports, fragments of data sets, or data without context.

Motel Voucher: Payment for motel lodging for a homeless individual or household for a short duration. Vouchers can be for one night or multiple nights.

Penetration Testing: The process of probing a computer system with the goal of identifying security vulnerabilities in a network and the extent to which outside parties might exploit them.

Permanent Supportive Housing: Long term, community-based housing that has supportive services for homeless persons with disabilities. This type of supportive housing enables special needs populations to live independently as possible in a permanent setting. Permanent housing can be provided in one structure or in several structures at one site or in multiple structures at scattered sites.

Privacy: (withdrawal from public view; of belong to or concerning a particular person; not open to, intended for, or controlled by the public, a.k.a. privacy protections) Privacy refers to protecting the rights of clients data and includes protection of the personal client information stored in the HMIS from open view, sharing or inappropriate use.

Public Data: Published information that has been approved for public release by the Summit County Continuum of Care and the HMIS Advisory Committee.

Public Key Infrastructure: Self-issued certificate authority (parties trust each other). Third party certificate authority (parties do not have historically trusting relationship).

Rental Assistance: (rent, security deposit) Short term rent assistance – usually 6 months or less and often only one month. Rental assistance provided to participants in Transitional or Supportive Housing should not be entered as part of a Rental Assistance program unless it is to assist the participant move into permanent housing.

Restricted Data: Information not ever scheduled for publication. Examples include data sets that are unassociated with any official project or data that have not been analyzed.

Security: (something that gives or assures safety; protection or defense against attack, interference, espionage; procedures to provide such protection) Protection of the client and program information stored in the HMIS from unauthorized access, use, or modification.

Shelter Plus Care Program: A program that provides grants for rental assistance for homeless persons with disabilities through four component programs: Tenant, Sponsor, Project, and Single Room Occupancy (SRO) Rental Assistance.

Supportive Housing: Similar to Transitional Housing below, except this program is funded through the Continuum of Care Supportive Housing Program (SHP).

Transitional Housing: A project that has its purpose facilitating the movement of homeless individuals and families to permanent housing within a reasonable amount of time (usually 24 months).

Transitional Shelter: Facility-based or scattered site units that provide a short-term period of transition from homelessness to transitional or permanent housing. Supportive services such as case management, housing counseling, money management, transportation, etc. may be provided. Guests may often stay in transitional shelter 6+ months before moving to transitional or permanent housing.

Written Consent: Written consent embodies the element of informed consent in a written form. A client completes and signs a document consenting to an understanding of the options and risks of participating or sharing data in an HMIS system. The signed document is then kept on file at the agency.