



Homeless Management Information Systems

**Policy & Procedures Manual
September, 2008**

I. HMIS Roles & Responsibilities Defined

a. 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:

- There will be a concerted effort to find replacement representatives when participation has been inactive or inconsistent from the organizations involved in the project;
- There will be a pro-active 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:

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

b. Info Line HMIS Administrator & Technical System Administrator staff

HMIS Administrator

HMIS Level of Access: System Administrator II

The Info Line, Inc. HMIS Administrator is the primary contact between the Akron/Summit County Continuum of Care, the HMIS Advisory Committee, and the HMIS Site Administrators.

Info Line, Inc. seeks to provide a secure and uniform HMIS which will yield the most consistent data for client management, agency reporting, and service planning. The HMIS Administrator will provide system-wide oversight and a single point of contact with the Akron/Summit County Continuum of Care and all participating community agencies. All system-wide questions and issues should be directed to this person.

Responsibilities include:

- Auditing usage and access of the database.
- Developing reports to present the data.
- Mining the database to respond to the information needs of participating organizations, community stakeholders and consumers.
- Documenting work on the database and in development of reports/queries.
- Provision of technical assistance as needed with program sites.
- Providing training and technical assistance to participating organizations on all policies and procedures authorizing access to the system including set-up, questions from users, network questions and system functionality questions.
- Coordinating technical support for system software.
- Oversight of all contractual agreements with funders, participating organizations, and consultants in adherence with the recommendations of the Summit County Continuum of Care.
- The daily operations including meeting project objectives; orientation of new staff to program operations, managing and updating the HMIS Policies and Procedures manual.
- Communicate with participating Organization leadership and other stakeholders regarding the HMIS project.
- Maintain a list of agency Site Administrators.
- Assuring data entry begins within 30 days of completed training.

System Administrator

HMIS Level of Access: System Administrator II.

The System Administrator's primary responsibility is hardware and software coordination and maintenance of the Akron/Summit County HMIS. A third party vendor, Amos Data Systems is designated as the backup support for this position. This position will also be the point of contact for Bowman Systems, Inc. software updates and installations, server backup and maintenance issues,

and maintaining the security of HMIS data storage. Info Line, Inc. will provide a highly available database server and will inform users in advance of any planned interruption in service.

HMIS Trainer

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 or Project Connect Instructors.

Hotline Support

Info Line, Inc. 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.

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

The support hotline will be staffed by the HMIS Administrator, the System Administrator, and an additional part-time HMIS Trainer. Level of HMIS Access may vary depending on who provides support.

c. 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 Info Line 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:

- 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.

- Will be held responsible for enforcing established policy for any misuse of the software system by his/her designated staff.
- Providing a single point of communication between the end users and the Info Line Technical staff around HMIS issues;
- Ensuring the stability of the agency connection to the Internet and ServicePoint, either directly or in communication with other technical professionals;
- Organizing initial and ongoing Training for their agency users;
- 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.
- Providing site support for the generation of agency reports;
- Managing agency user licenses; and
- Monitoring compliance with standards of client confidentiality and ethical data collection, entry, cleansing and retrieval.
- 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.
- 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.
- Notifying all users in their agency of interruptions in service.
- Ensure data entry commences in the live system within thirty (30) days after receiving the appropriate training(s).
- Ensure that all data entry is completed in the live system for each program within fifteen (15) days from intake.

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

d. **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 Info Line HMIS Administrator via e-mail or phone.

Responsibilities of the agency staff:

- To be aware of the data's sensitivity and take appropriate measures to prevent unauthorized disclosure.
- For reporting security violations.
- For complying with all Policies and Procedures.
- For their actions and for any actions undertaken with their usernames and passwords.
- Ensure data entry commences in the live system within thirty (30) days after receiving the appropriate training(s).
- Ensure that all data is being entered into the HMIS within fifteen (15) days from intake.

II. Personal User Identification and Passwords

a. **Access Privileges and Levels to System Software**

- Access to the Summit County Homeless Management Information System will be controlled based on the user's needs. Need exists only for those system administrators, shelter staff, volunteers, or designated personnel who work directly with (or supervise staff who work directly with) clients or have data entry responsibilities.
- 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.
- An agency or an individual user's access may be suspended or revoked for suspected or actual violation of the security protocols.
- Only authorized computers with registered Citrix licenses will be able to access the HMIS system from authorized locations. Computers must be specifically identified by the Executive Director of the Participating Agency and HMIS Administrator. Access by an unauthorized computer will be considered a security violation.

b. Access to Client Paper Reports generated from System

- Printed versions of confidential data should 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.
- Responsible personnel must authorize the shipping and receiving of magnetic media, and appropriate records must be maintained.
- Authorized employees using methods deemed appropriate by the participating agency may transport HMIS data that meet approved security standards.
- Reasonable care should be used, and media should be secured when left unattended. Magnetic media containing HMIS data that is released and/or disposed of from the Participating Agency and Central Server should first be processed to destroy any data residing on that media. Degaussing and overwriting are acceptable methods of destroying data.
- HMIS information in hardcopy format should be disposed of properly. This may include shredding finely enough to ensure that the information is unrecoverable.
- All client records containing identifying information that are stored within the participating agency's local computers are the responsibility of the participating agency.

c. Unique User ID's and Passwords

- **Access Levels:** Participating Agencies will manage the proper designation of user accounts to enforce aforementioned information security protocols. All agency access levels will be determined and approved by the Executive director of the participating agency in consultation with the HMIS Administrator. User access levels will be directly related to the user's job responsibilities and approved need for access to the HMIS. The HMIS Administrator will generate a username and password for the Agency administrator who will then generate usernames and passwords for agency users.

Resource Specialist I 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. A Resource specialist cannot modify or delete data.
Resource Specialist II 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.
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.

- **Passwords:** User accounts will be created and deleted by the Info Line HMIS Administrator under the authorization of the Agency's Executive Director. The user will be required to change the password the first time they log onto the system. The password must be between 8 and 16 characters and contain 2 numbers. Passwords are the individual's responsibility and users cannot share passwords. Passwords should not be easily guessed or found in any dictionary and should be securely stored and inaccessible to other persons. The password is alphanumeric. Passwords expire every 45 days. A password cannot be re-used until one entirely different password selection has expired.
 - **Sharing Data between Agencies:** Users will only be able to view the data entered by users of their own agency. Agencies are restricted from viewing each other's information unless specific sharing agreements have been negotiated in advance and the client has given written consent.
 - **Termination:** The Agency Administrator should terminate the rights of a user immediately upon termination from their current position. If a staff person is to go on leave for a period of longer than 45 days, their password should be inactivated within 5 business days of the start of their leave. The Agency Administrator is responsible for removing users from the system. The Agency Administrator must update the access list and signed agreement on a quarterly basis and provide any changes to the HMIS Administrator.
- d. **Auditing – Monitoring, Violations and Exceptions, Data logs**
- The Agency Administrator will be responsible for monitoring all user access within their own agency. Any violations or exceptions should be documented and forwarded to the HMIS Administrator immediately. All data or system security and/or confidentiality violations will incur immediate individual user access suspension until the situation is effectively resolved.
 - Participating Agencies may request an Exception to the security and privacy standards. All exceptions must be approved by the HMIS Advisory Committee. However, in lieu of an approved Exception, participating Agency or a user access may be suspended or revoked for suspected or actual violation of the security protocols.
 - Serious or repeated violation by users of the system may result in the suspension or revocation of an agency's access.
 - All exceptions of these standards are to be requested in writing by the Executive Director of the Participating Agency. Any exception to the data security policies and standards not approved by the HMIS Advisory Committee is a violation.

- All potential violations of any security protocols will be investigated.
- 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.
- Any agency that is found to have consistently and/or flagrantly violated security protocols may have their access privileges suspended or revoked.
- 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.

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.

- 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 Info Line, Inc.
- 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 Info Line, Inc. All participating agency staff must complete all user participation forms.
- 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 Info Line. If the agency terminates participation in the HMIS project, all hardware provided will be returned to Info Line. Consulting time spent to reconfigure software setup to access HMIS will be charged to the agency at the current Info Line consulting

rate.

- d. **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.
- e. **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.)
- f. **Logon and Data 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 Info Line 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.
- g. **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.
- h. **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.
- i. **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.
- j. **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.

k. Reassessment and Monitoring:

- i. The HMIS Administrator will run ongoing training to address any agency staff turnover issues, or additional training and support that may be needed.
- ii. 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.
- iii. Performance will be tracked by the Agency Administrator and evaluated with the HMIS Administrator for areas to improve the process if needed.
- iv. 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.

IV. Technical Support and Other Support

a. System Availability

The intent of Info Line, Inc. 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 Info Line 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 Info Line HMIS Administrator will contact the Agency Site Administrators and inform them of the cause and duration of the interruption in service.

b. 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 Info Line, provides computer hardware, the agency is still responsible for maintaining their own Internet connection. Info Line 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 Info Line, Inc. 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 Info Line where the hardware has been provided by Info Line.

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.

c. Info Line Technical support (when, response time)

Info Line, Inc. 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 Info Line 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.

d. Grievances

Agency Grievances

Any problems related to the operation or policies of the Akron/Summit County HMIS should be directed to Info Line, Inc. 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 Info Line, Inc. 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 Info Line, Inc. through the HMIS Administrator. If Info Line, Inc. cannot resolve the problem, the Info Line 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 Info Line HMIS staff will be available to discuss and resolve agency HMIS problems. If a problem is not satisfactorily resolved by Info Line, Inc., 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 Info Line 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. Info Line, Inc. 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 Info Line 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

- a. **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.
- b. **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)

- Citrix license
- Windows CAL & Terminal Server License
- Bowman ServicePoint License
- Bowman Support
- Bowman Security Software License
- Bowman Security Support

Optional Microsoft Office, File Storage, Back-Ups on Info Line’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 Info Line, Inc. for current pricing information.

- c. **Maintenance of onsite computer equipment:** Computer equipment provided by Info Line 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 Info Line Citrix mainframe.

Minimum Computer requirements:

- 5. Pentium PC
- 6. Operating system: Windows 98, Windows 2000, Windows XP
- 7. Internet Connectivity

- d. **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.
- e. **Additional user license requests**

The Agency Administrator should obtain a User License Request Form. This form can be downloaded from the HMIS website at www.HMISSummit.net, then click on the forms tab.

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 Info Line 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 Info Line HMIS Administrator for price information.

All new users MUST complete training and assessments before they can receive an HMIS ID and Password.

f. 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

a. Inter-Agency Data Sharing:

1. Personal Identifying Data entered into the Akron/Summit County HMIS by participating agencies will be only be accessible to the agency who entered the client's data.
2. All participating agency profiles will be initiated with a Closed Security status within the ServicePoint software.
3. 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.
4. Participating agencies will specify the data sections that will be shared with the other identified agencies who wish to share the same client data.
5. 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.

b. Client Consent:

1. 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 a closed status will be assumed.
2. All participating agency profiles will be initiated with a Closed Security status within the ServicePoint software.
3. 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.

4. 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

- a. **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.
- b. **Data Integrity Expectations:** Participating agencies will provide the following levels of accuracy and timeliness:
 1. All names will be accurate;
 2. All required data fields will not exceed 5% null response per month;
 3. All services provided will be compatible with the providing program;
 4. In all reports of shelter provided for a client, the client must be eligible to receive shelter services from the listed provider; and
 5. Data entry for all services provided during one calendar month must be entered into the HMIS 15 days from the date of intake whenever it is not reliant on another agency's intake process (i.e. an AMHA issued voucher).
- c. **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.
- d. **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.

e. Public:

1. 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.
2. All requests for data from anyone other than a Participating Agency or client will be direct to the HMIS Administrator at Info Line, Inc. 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.

f. Data Retrieval Support:

1. Participating agencies will create and run agency-level reports.
2. 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 Info Line, Inc., 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 of 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. Info Line 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. Info Line, Inc. 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 Info Line in Akron, Ohio. 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

Info Line secures the perimeter of its network using Cisco PIX 515 E Security Appliances. Firewall services that protect Info Line's network from threats lurking on the Internet. The firewall provides real-time, in-line monitoring, interception, and response to network misuse through broad support for the most common attack intrusion detection signatures. These intrusion detection capabilities enhance the Cisco PIX Security Appliance's best-of-breed stateful inspection firewall features by providing an additional layer of network protection. Appropriate action can be taken on packets and traffic flows that violate a security policy or represent malicious network activity.

SSL Data Encryption

The SSL (Secure Sockets Layer) Handshake Protocol is able to negotiate encryption keys as well as authenticate the server before data is exchanged by the higher-level application. The SSL protocol maintains the security and integrity of the transmission channel by using encryption, authentication and message authentication codes.

This is how the process works at Info Line:

The SSL Handshake Protocol consists of a server authentication and a client authentication. The server, in response to a client's request, sends its certificate and its cipher preferences. The client then generates a master key, which it encrypts with the server's public key, and transmits the encrypted master key to the server. The server recovers the master key and authenticates itself to the client by returning a message authenticated with the master key. Subsequent data is encrypted and authenticated with keys derived from this master key. In the optional second phase, the server sends a challenge to the client. The client authenticates

itself to the server by returning the client's digital signature on the challenge, as well as its public-key certificate.

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 and database connection level for additional security. Users are required to access the ServicePoint™ application by first signing on to an Info Line Citrix server with an individual ID and password.

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. Info Line 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 Info Line 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 Info Line 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 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 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 I.D. 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:

- 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.
- Keep a record of this client's anonymous I.D. 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 for is completely voluntary. 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 Info Line, Inc. 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 CITRIX and ServicePoint user license, the Agency is required to adhere to the following participation requirements:

- All users must complete HMIS training and an HMIS User Agreement form to be granted live system access.
- 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.
- 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.
- 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.
- No more than 1 user can be assigned to a ServicePoint license at one time.
- 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. 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.