



Buffalo Area Services Network
Homeless Management
Information System

Standard Operating Procedures Manual

May 2006

**Buffalo Area Services Network (BAS-Net)
Homeless Management Information System
Standard Operating Procedures Manual**

Table of Contents

I. Introduction	3
II. Roles and Responsibilities	
Bowman Internet Systems	5
Homeless Alliance of Western New York	5
Homeless Alliance of Western New York Board of Directors	5
BAS-Net Advisory Committee	5
BAS-Net Administrator	6
BAS-Net Support Specialist	6
BAS-Net Site Contact	7
BAS-Net Agency Users	7
III. BAS-Net Policies and Procedures	
Participation	8
Equipment, Licensure, and Software Applications	9
Support	11
Security	13
Security Incident Reporting	17
System Access	19
Agency Readiness Assessment and Training	25
Inter-Agency Data Sharing	28
Client Informed Consent and Release of Information	29
Data Collection, Types, and Usage	33
Data Quality and Control	35
Data Ownership	36
Grievances	37
Termination of Participation	39
Use of Unnamed Client Feature	41
IV. Supporting Documents	
Agency Partner Agreement	44
Inter-Agency Data Sharing Agreement	54
User Policy, Responsibility Statement, and Code of Ethics	56
Client Consent and Release of Information Authorization	58
Client Consent and Release of Information Authorization (HIPPA)	59
Consumer Notice	62
Privacy Protection Notice	63
User License Request	64
Grievance Form	65
Security Incident Report	66
Revocation of Consent Form	68
V. Glossary of Terms	69

I. Introduction

The Buffalo Area Services Network (BAS-Net) is a Homeless Management Information System which allows authorized personnel at homeless housing and service provider agencies to enter, track, and report information on the clients they serve. Using Internet-based technology, BAS-Net provides opportunities for service providers to improve coordinated care to homeless persons in the Buffalo and Erie County area while meeting reporting requirements for the U.S. Department of Housing and Urban Development (HUD) and other funders.

In compliance with all federal requirements regarding client confidentiality and data security, BAS-Net is designed to collect and deliver timely and accurate data about services and homeless persons or persons at risk for being homeless. This information is collected via interviews conducted by trained service provider staff. Data is then analyzed in order to provide an unduplicated, aggregate count (void of any identifying client-level information). This information is made available to service providers, advocates, consumer representatives, and policy-makers. Information is also used to better understand current gaps in the homeless continuum of care and human service delivery system.

BAS-Net utilizes the ServicePoint Client Information Management System developed by Bowman Internet Systems. ServicePoint is an Internet-based client information system that provides a standardized assessment of consumer needs, aids in the creation of individualized service plans, and records the use of housing and services. Communities can then use this information to determine how services are utilized, identify service needs, and develop outcome measurements.

Involvement in the BAS-Net system will allow service providers to generate automated APRs and reports which can aid in the development and evaluation of programming. At a community level, BAS-Net will provide aggregated data across the entire homeless service continuum for use in the annual Continuum of Care funding application and city and county consolidated plans. Findings can also be used to inform policy decisions aimed at addressing and ending homelessness at the local, state, and federal levels. Finally, and most importantly, BAS-Net will ease the process of securing services for homeless individuals and families in our area. A more complete list of the potential benefits of BAS-Net is available on the page that follows.

This document provides information about BAS-Net staffing, technology, and participation requirements, as well as an overview of policies, procedures, and standards that govern its operation especially with regard to confidentiality, security, and data expectations. Copies of all necessary supporting documents are also included in this manual as well as a glossary of commonly-used terms.

Potential Benefits of BAS-Net

For Homeless Persons	For Service Providers	For Community
Makes it possible to maintain intake information over time so the number of times a homeless person repeats their story to providers is reduced.	Provides real-time information about needs and available services for homeless persons.	Helps the community to define and understand the extent of homelessness throughout Buffalo and Erie County.
Offers an opportunity to conduct intakes and life histories once; illustrating that service providers consider the homeless person's time valuable and ensuring consumer dignity.	Assures confidentiality by keeping information in a secured system.	Provides greater focus for staff and financial resources to the geographical areas, agencies, and programs where services for the homeless are needed most.
Makes it possible to coordinate multiple services and streamline referrals. This will help to reduce consumer waiting time.	Decreases duplicative client intakes and assessments.	Allows for better evaluation of the effectiveness of specific interventions, programs, and services.
	Tracks client outcomes and provides a client history.	Offers local, state, and federal legislators data and information about the homeless population.
	Generates data reports for local use and to meet state and federal requirements.	Makes it possible to meet all federal reporting requirements.
	Facilitates the coordination of services internally and externally with other agencies and programs.	
	Provides access to a community-wide database of service providers and allows agency staff to easily select a referral agency.	

II. Roles & Responsibilities

Bowman Internet Systems	<p>Responsible for the delivery of Internet-based client assessments and reporting features.</p> <p>Bowman Internet Systems will provide secure, on-going access to its ServicePoint, ShelterPoint, and ResourcePoint applications via the Internet. In addition, Bowman Internet Systems will also provide information about any system modifications and/or upgrades.</p>
Homeless Alliance of Western New York (HAWNY)	<p>Responsible for the administration and staffing of BAS-Net.</p> <p>HAWNY will secure funding for the BAS-Net system and provide organizational oversight through its Board of Directors and the BAS-Net Advisory Committee. HAWNY will also provide regular staffing for the project.</p>
HAWNY Board of Directors	<p>Responsible for providing organizational oversight for the BAS-Net system through review of policy and procedures identified by the BAS-Net Advisory Committee.</p>
BAS-Net Advisory Committee	<p>Responsible for developing and reviewing all system-wide policies and procedures for BAS-Net.</p> <p>In selecting participants for this committee, HAWNY will attempt to secure and maintain representation from each:</p> <ul style="list-style-type: none"> • Homeless housing and service type; • HUD-identified homeless subpopulation; • Continuum of Care municipality; and from • Current and formerly homeless individuals <p>The BAS-Net Advisory Committee will provide input on an on-going basis for the local HMIS project. The Committee will share its recommendations with the HAWNY Board of Directors on the key issues that follow:</p> <ul style="list-style-type: none"> • Determining guiding principles for BAS-Net; • Selecting data elements to be collected by participating agencies; • Defining parameters for the release of aggregated HMIS data; • Evaluating compliance with HUD data and technical standards; • Reviewing the HMIS-related performance of participating agencies especially adherence to local policies and procedures; and • Addressing issues that arise from use of BAS-Net including, but not limited to, client grievances and policy adjustments.

<p>BAS-Net Administrator</p>	<p>The BAS-Net Administrator is responsible for the implementation and coordination of the local HMIS. The administrator will be the primary contact for HAWNY, the BAS-Net Advisory Committee, and BAS-Net Site Contacts.</p> <p>Responsibilities include:</p> <ul style="list-style-type: none"> • Orienting prospective BAS-Net participants to system; • Maintaining a list of agency contacts and BAS-Net participants; • Providing oversight on all contractual agreements; • Assessing agency readiness for HMIS; • Providing regular trainings (SOP/Confidentiality/Applications); • Authorizing access to the BAS-Net system (Set-Up); • Developing client assessment tools not already included; • Providing basic technical assistance to participating agencies; • Facilitating access to hardware/other technical support; • Documenting database and policy/procedure changes; • Developing and evaluating performance objectives; • Updating “Standard Operating Procedures Manual;” • Monitoring, reporting, and resolving access control violations; • Auditing BAS-Net usage system-wide; • Developing reports and queries for Continuum of Care; • Presenting research findings to community stakeholders; • Coordinating regular user-group meetings; and • Communicating with participating agencies/larger community.
<p>BAS-Net Support Specialist</p>	<p>The BAS-Net Support Specialist’s primary responsibility is hardware and software coordination and maintenance for the local HMIS. The support specialist will serve as a secondary contact for HAWNY, the BAS-Net Advisory Committee, and BAS-Net Site Contacts.</p> <p>Responsibilities include:</p> <ul style="list-style-type: none"> • Orienting partner agencies to BAS-Net by demonstrating HMIS functions and features, assisting in training sessions, and assessing HMIS readiness; • Providing computer support and technical assistance to partner agencies to ensure appropriate use of HMIS; • Tracking and resolving problems reported by agency users and perform follow-up on outstanding problems; • Assisting with the coordination of data integration, conversion and programming modification tasks with participating agencies and vendors to facilitate an integrated multi-agency database; • Identifying and developing needed training materials; and • Participating in user meetings to address on-going system enhancements, facilitate information sharing, and identify best practices.

<p>BAS-Net Site Contact</p>	<p>The BAS-Net Site Contact will serve as the agency contact for the project and will facilitate access to the HMIS at an organizational level.</p> <p>Each BAS-Net Site Contact will be responsible for:</p> <ul style="list-style-type: none"> • Participating in HMIS readiness assessment; • Identifying BAS-Net users and facilitating access to training; • Granting BAS-Net access only to authorized staff members that have received training and demonstrated proficiency in application use and understanding of policies and procedures; • Monitoring staff compliance with standards of client confidentiality and ethical data collection, entry, cleaning, and retrieval and enforcing established misuse policy; • Enforcing business controls and practices to ensure organizational adherence to policies and procedures including detecting and responding to violations; • Providing on-site support for the generation of agency reports and managing user licenses; • Ensuring stability in the agency Internet connection either directly or in communication with a technician; and • Notifying users about interruptions in service. <p>Each agency must designate a primary BAS-Net Site Contact at each program location to increase effectiveness of communication both between and within agencies.</p>
<p>BAS-Net Agency Users</p>	<p>BAS-Net Agency Users are responsible for entering client data into the system as well as identifying needs and concerns regarding HMIS to their Site Contact.</p> <p>BAS-Net Agency Users will be responsible for:</p> <ul style="list-style-type: none"> • Being aware of the confidential nature of data and taking appropriate measures to prevent any unauthorized disclosure of client information; • Complying with all local HMIS policies and procedures; and • Reporting security violations to their BAS-Net Site Contact. <p>Agency users are also responsible for their own actions or any actions undertaken with their usernames and passwords.</p>

III. Policies and Procedures

Participation

Policy: The BAS-Net Advisory Committee will establish requirements for participation in the local HMIS. All requirements for participation will be outlined in the BAS-Net Standard Operating Procedures Manual.

Participation in BAS-Net is required of all HUD-funded homeless service providers in the Buffalo and Erie County area. Programs that receive financial support from the HUD Emergency Shelter Grant (ESG), Supportive Housing (SHP), Shelter Plus Care (S+C), Section 8 Moderate Rehabilitation for SRO, or Housing Opportunities for Persons with AIDS (HOPWA) are expected to fully participate in the data collection as per federal requirements. Homeless service and housing providers not funded by HUD are **STRONGLY ENCOURAGED** to participate. In order to participate in BAS-Net, providers must agree to each of the following:

Participation Agreement: Agencies are required to sign a participation agreement stating their commitment to adhere to the policies and procedures for effective use of BAS-Net and proper collaboration with HAWNY. A copy of the Agency Partner Agreement is available in the Supporting Documents section of this manual and on the HAWNY website.

Identification of BAS-Net Site Contact(s): Agencies will designate one or more key staff persons to serve as BAS-Net Site Contact(s). Site Contacts will be responsible for creating usernames and passwords and monitoring access to the system. The site contact will also be responsible for reporting any system-or computer-related problems to the BAS-Net Administrator and Support Specialist.

Training: BAS-Net Site Contacts will be responsible for identifying BAS-Net users and facilitating their access to initial and any subsequent training sessions. Each new designated user must attend a training prior to gaining access to the system. They must also sign the User Policy, Responsibility Statement, and Code of Ethics form and forward the form to the HAWNY office. A copy of this form is available in the Supporting Documents section of this manual and on the HAWNY website.

On-Going Information Sharing: Agencies must agree to send at least one representative to regularly attend user meetings. This representative is responsible for disseminating information to other agency BAS-Net users.

Client Consent: Agencies will maintain signed copies of the Client Consent and Release of Information Authorization Form in a secure, on-site location. These forms authorize the input of personal information electronically into BAS-Net and specify what information may be included. A copy of the form should be provided to each client.

Data Collection: Agencies agree to collect client information on all HUD- and locally-required data elements. HUD-required elements are identified through Data and Technical Standards. Local elements will be established by the Advisory Committee.

Equipment, Licensure, and Software Applications

Policy:	The BAS-Net Advisory Committee will establish equipment requirements for participation in the local HMIS. All requirements for equipment will be outlined in the BAS-Net Standard Operating Procedures Manual.
----------------	--

BAS-Net Computer Equipment: As part of the BAS-Net start-up grant, the Homeless Alliance of Western New York (HAWNY) has secured funds to provide each participating site with one (1) desktop computer and three (3) ServicePoint user licenses. In addition, HAWNY will provide DSL Internet-connection and service, security locks, and anti-virus software and updates over the life of the grant. Equipment purchased through the BAS-Net start-up grant is considered property of HAWNY and must be returned if the agency decides to terminate participation in the system.

A list of workstation minimum requirements and bandwidth recommendations follows for participating agencies who are interested in using their own equipment to access the BAS-Net system.

Workstation Computers

- Pentium Class PC
- Operating System: Windows 98 or higher
- 128mb RAM
- Microsoft Internet Explorer 5.5 or higher, or Netscape Navigator 6 +
- 128-bit cipher encryption on Browser
- Browser cache set to “Check for new version: Every visit to page.”
- Broadband Internet Connection (hosted version) or LAN connection.
- Up-to-Date Anti-Virus Protection

Bandwidth Recommendations

The average user will need to sustain a 30-50 kb per second download throughput to effectively use the BAS-Net Site.

Communication Equipment	Comments
56K Modem	Not recommended.
SDSL 512Kbps/62.5KB/s	Allows eight users to concurrently browse the BAS-Net Site or use the Internet.
ADSL 1.5-8Mbps/ 187.5KB/s-1MB/s	Allows 125 users concurrently to use the BAS-Net site or use the Internet.

Cable 1Mbps/122.1KB/s	Allows 15 users to concurrently use the BAS-Net site or the Internet.
T1 1.544Mbps/ 188.5KB/s	Allows 23 users to concurrently use the BAS-Net site or the Internet.
T3 44.763Mbs/ 5.461MB/s	Allows 682 users to concurrently use the BAS-Net site or the Internet.

Maintenance of Computer Equipment: Computer equipment provided through BAS-Net will be supported by the HAWNY staff and through contract with Dell Computers as long as the integrity of the initial physical setup is maintained. Under no circumstances should program staff remove the cover from the computer tower. Doing so will void the computer support contract with Dell Computers.

BAS-Net staff will be responsible for the initial setup of each computer system. Computer equipment owned by each agency will be maintained and supported by the agency.

Additional Licenses: The Homeless Alliance of Western New York (HAWNY) provides a minimum of 3 user licenses upon original setup. Participating Agencies can purchase additional user licenses through HAWNY if desired. To do so, the BAS-Net Site Contact must complete a User License Request Form. A 1-year commitment is required. License costs may vary due to vendor product price changes. Agencies interested in purchasing licenses should contact HAWNY for current price information. A copy of the User License Request Form is available in the Supporting Documents section of this manual and on the HAWNY website.

Customization Requests: All on-site BAS-Net Site Contacts have the ability to customize the agency profile, reset passwords, and customize reports. In the event that an additional assessment is needed in order to collect client data, a written request should be sent to the BAS-Net Administrator detailing the customization requested and the date needed. Requests will be addressed on a first come, first served basis.

Support

Policy: The BAS-Net Advisory Committee will establish guidelines regarding system and computer support and maintenance for the HMIS. These guidelines are outlined in this Standard Operating Procedures Manual.

System Availability: The BAS-Net system is available 24 hours a day, 7 days a week, 52 weeks a year with the exception of scheduled system back-ups and routine maintenance.

- *In the event of planned downtime*, the BAS-Net Administrator will inform agencies via electronic mail, fax, or telephone. Announcements about planned system outages will also be broadcast via the System-wide NewsFlash feature in BAS-Net.
- *In the event of unscheduled downtime*, the BAS-Net staff will contact the BAS-Net Site Contact at each location to inform them of the cause and possible duration of the service interruption. Contact will be made via electronic mail, fax, or telephone.

Support: The BAS-Net Staff will provide system support by phone, electronic mail, computer shadowing, and/or in-person consultations. The BAS-Net Site Contact should act as the first level of contact when a system problem arises and should determine if the problem requires immediate rectification.

- *If the BAS-Net Site Contact cannot resolve the problem and immediate assistance is needed*, the Site Contact should call BAS-Net staff on their cell phone and leave a contact number. BAS-Net staff will respond to the call as soon as possible. BAS-Net System Administration emergency contact information will be given to each Site Contact and Licensed User.
- *If the BAS-Net Site Administrator cannot resolve the problem and assistance is not immediately needed*, the Site Contact should utilize the Trouble Ticket feature, which can be accessed through the BAS-Net Information Page on www.wnyhomeless.org. BAS-Net staff will phone or email the site contact and arrange for needed assistance.

It is the goal of the BAS-Net Staff to respond to all participating agency needs within one business day of initial contact.

Technical: BAS-Net staff will provide technical support on any hardware provided to the agency as part of the initial BAS-Net grant as long as the agency maintains the integrity of the initial physical setup. BAS-Net staff will not support hardware or software not part of the initial program set-up. Any fees incurred to fix problems related to added hardware or software will be charged to the agency.

For some computer problems, it may be necessary for the BAS-Net Staff to receive special assistance from Dell Computers. As part of the BAS-Net Contract, HAWNY has secured "Gold Support" coverage from Dell which includes 24/7 technical support. The BAS-Net staff will make any necessary contact with Dell and will coordinate activities with participating agency and Dell Technicians. Under no circumstances should program staff remove the cover from the computer tower. Doing so will void the computer support contract with Dell Computers.

Participating agencies using their own computer hardware and Internet connections will be responsible for providing their own technical support on their own equipment.

Maintenance: BAS-Net staff will provide maintenance on any hardware provided to the agency as part of the initial BAS-Net grant as long as the agency maintains the integrity of the initial physical setup. Maintenance includes regular system checks (e.g., hard drive defragmentation) as well as anti-virus and spy-ware updates.

BAS-Net staff will call Site Contacts to schedule a convenient time for maintenance to take place. In most circumstances, maintenance will be done when few users are on the system to reduce the likelihood of interruption.

Participating agencies using their own computer hardware and Internet connections will be responsible for providing maintenance on their own equipment.

Security

Policy:	Access to all of central server computing, data communications, and sensitive data resources will be 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. BAS-Net staff will work to ensure that all sites receive the security benefits of the system while complying with all stated policies.
----------------	--

Security – Bowman Internet Systems

Physical Security: Bowman Internet Systems (BIS) hosts the central server for the BAS-Net system. The BIS data center is located at its headquarters in Shreveport, Louisiana. Located in a 20-story office complex, 24-hour security is provided. After normal business hours, card access is required and monitored. In addition, separate, limited key access is required for entry into the main office and into the server room.

Access to Server: No one will have direct access to the BAS-Net system through any means other than ServicePoint software unless explicitly given permission by the BAS-Net Administrator during a process of maintenance, software upgrade, or conversion. BIS will monitor access to the BAS-Net server and employ security methods to prevent unauthorized database access. 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.

Firewall Protection: BIS secures the perimeter of its network using technology from firewall vendors. The firewall provides real-time, in-line monitoring, interception, and response to network misuse through broad support for the most common attach intrusion detection signatures. Appropriate action can be taken on packets and traffic flows that violate a security policy or represent malicious network activity. Company system administrators monitor firewall logs to determine unusual patterns and possible system vulnerabilities.

SSL Data Encryption: BIS utilizes commercial-grade, 128-bit SSL encryption for data traveling over the Internet to the BIS network. The SSL (Secure Sockets Layer) Handshake Protocol negotiates encryption keys and authenticates 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.

The SSL Handshake Protocol consists of a server and 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.

As a user enters ServicePoint, they access data with 128-bit encryption from their browser and 1024-bit RSA public key from the ServicePoint servers. Distinguished by a lock icon in the corner of their browser, users are ensured that their data is secure in transit.

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 four consecutive times, ServicePoint automatically marks them inactive. For added security, the session key is automatically scrambled and re-established in the background at regular intervals.

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: All database access is controlled at the operating system and database connection levels for additional security. Access to production databases is limited to a minimal number of points; as with production servers, production databases do not share a master password database.

Security - Homeless Alliance of Western New York and BAS-Net

Physical Security: The Homeless Alliance of Western New York is housed at 2211 Main Street. Access to the building is monitored via a swipe card and/or staff security. Passwords are required to access individual workstations. Any raw data or system information is stored in locked cabinets to maintain confidentiality and security.

System Administrator Access: Access to all computing, data communications, and data resources will be controlled. Access is controlled through user identification and authentication. The BAS-Net Administrator is responsible and accountable for the work done under personal identifiers. Access control violations must be monitored, reported and resolved.

System Access Monitoring: BAS-Net automatically tracks and records access to every client record by use, date, and time of access. BAS-Net staff will monitor access to system software by regularly reviewing user access privileges and removing identification codes and passwords when users no longer require access. BAS-Net staff will audit all unauthorized accesses and attempts to access information. Audit records shall be kept at least six months according to industry standards.

User Authentication: BAS-Net will only be accessed with a valid username and password combination, which is encrypted via SSL for Internet transmission to prevent theft. If an administrator enters an invalid password four consecutive times, BAS-Net automatically marks them inactive. For added security, the session key is automatically scrambled and re-established in the background at regular intervals.

Administration and System-wide Data: The BAS-Net Administrator will have full access to BAS-Net. The administrator can add, edit, and delete users, agencies, and programs and reset passwords. Access to system-wide data will be granted based upon need to access the data and with the approval of the BAS-Net Advisory Committee.

Data Usage and Protection: See Data Collection, Types, and Usage.

Data Security: Wherever possible, all database access is controlled at the operating system- and database-connection level for additional security. Only the BAS-Net Administrator will have access to changing database information at the server level. When this is done, an appropriate written summary of the information changed will be logged by the BAS-Net Administrator. The BAS-Net Administrator will produce a bi-monthly report to be overseen and audited by the BAS-Net Advisory Committee.

Security – Participating Agencies

Physical Security: Agencies must develop rules to address physical access to workstations. Monitors displaying client data must be oriented to minimize viewing by unauthorized persons.

User Authentication: BAS-Net will only be accessed with a valid username and password combination, which is encrypted via SSL for Internet transmission to prevent theft. If a user enters an invalid password four consecutive times, BAS-Net automatically marks them inactive and requires that they contact their BAS-Net Site Contact for reactivation. If the Site Contact is unavailable, the staff member should contact the BAS-Net Administrator and will be asked a security question to confirm their identity. For added security, the session key is automatically scrambled and re-established in the background at regular intervals.

Access to Data - User Access: Users will only be able to view the data entered by users of their own agency or shared client records. BAS-Net has security measures in place which prohibit agencies from viewing each other's data.

Access to Data - Raw Data: Users who have been granted access to the BAS-Net Report Writer tool have the ability to download and save client level data onto their local computer. Once this information has been downloaded from BAS-Net in raw format to an agency's computer, these data then become the responsibility of the agency. Partner Agencies must develop protocols regarding the handling of data downloaded from Report Writer, record disclosure, and storage.

Access to Data - Policies Restricting Access to Data: Each BAS-Net participating agency must establish internal access to data protocols. These policies should include who has access, for what purpose, user account sharing and how they can transmit this information. Issues to address include storage, transmission, and disposal of data.

Client Paper Record Protection: Partner agencies must establish procedures to handle client paper records. Issues to be addressed include:

- Identifying which staff has access to client paper records and for what purpose;
- Allowing staff access only to the records of clients whom they work with or for data entry purposes;
- How and where client paper records are stored;
- Length of client paper record storage and disposal procedures; and
- Disclosure of information contained in client paper records.

Data Usage and Protection: See: Data Collection, Types, and Usage.

Security Incident Reporting

Policy: Participating agencies will report any occurrence that jeopardizes the security or functioning of the BAS-Net System so that appropriate measures can be taken to reduce risk and the likelihood of reoccurrence. BAS-Net Staff will be responsible for reporting security incidents to necessary authorities and to HAWNY Executive Director.

Defining a Security Incident: A security incident is defined as any occurrence that adversely affects or has the potential to adversely affect the integrity and/or confidentiality of the information contained within BAS-Net or its operation.

Categories and Definitions: Security incidents can be categorized as the following:

Category	Definition
Data or file extraction	Unauthorized, electronic removal of information from BAS-Net System.
Introduction of Malicious Code or Virus	Intentional or unintentional, unauthorized introduction of malicious code or virus onto the BAS-Net or agency computer equipment.
Modification of agency information	Intentional or unintentional, unauthorized modification of agency information.
Attempts to modify passwords or access rights	Intentional or unintentional attempt to modify BAS-Net user passwords or access rights.
Compromised or lost password	A compromise in a password occurs when staff believes that an individual other than the one to which the password is assigned becomes aware of the password. Sharing a password, except to BAS-Net Staff, is considered a compromise.
Theft of BAS-Net equipment or media	This includes stolen PCs, towers or media that may contain client information
Dissemination of protected client information from BAS-Net system in electronic or paper form	Intentional or unintentional, unauthorized dissemination of client information in an electronic format. This includes sending email or a FAX to an unintended recipient or sending of email in an unprotected manner. (i.e., through an unsecured mechanism)

Security Incident Documentation: All security incidents must immediately be reported to the BAS-Net Administrator via phone call. The BAS-Net Administrator will provide direction as needed to the individual(s) responding to the security incident and to evaluate the necessity of mobilizing additional resources. The BAS-Net Administrator is also responsible for ensuring that immediate action is taken to protect the security and integrity of the BAS-Net System and client data.

After the security incident, the staff member must complete a written Security Incident Report as soon as possible and forward it to the BAS-Net Administrator. The purpose of the report is to provide subsequent readers with an accurate image of the security incident through written documentation.

The report should be written in a clear, concise, and specific manner and should focus on the facts and events that occurred immediately prior to the incident, the incident itself, and the events that occurred immediately after the incident.

In addition to the above items, the report should include:

- Parties involved including each staff member's full name;
- A summary of each party's actions;
- Time and location of the incident; and
- Observations of any environmental characteristics that may have contributed to the incident.

The BAS-Net Administrator will take responsibility for reporting the incident to the HAWNY Executive Director, and when appropriate, law enforcement officials.

Review of Security Incidents: Security incidents will be reviewed at the next regularly scheduled meeting of the BAS-Net Advisory Committee to ascertain if the incident could have been avoided or the impact minimized. Each incident will be scrutinized to determine the appropriateness of staff actions and protocols. Recommendations about the need for additional resources, staff training, security modifications, and protocols will also be noted.

More specifically, the Advisory Committee will:

- Evaluate the timeliness, thoroughness, and appropriateness of the staff member's response to the security incident;
- Ascertain if the security incident could have been prevented;
- Recommend corrective actions, if warranted;
- Evaluate security incidents for trends and patterns;
- Monitor the agency's compliance with the security policies and protocols;
- Monitor the implementation of any preventative or corrective action; and
- Recommend changes to the HAWNY Board of Directors regarding policies, procedures and practices, and working agreements that will reduce the likelihood that similar security incidents would occur.

An aggregate report of security incidents will be compiled by the BAS-Net Administrator on a quarterly basis for review by the BAS-Net Advisory Committee. At minimum, these incidents will be analyzed by type of incident, location, employee/organizational involvement, time and date. Records of security incidents will be maintained by the BAS-Net Administrator.

Training around Security Incidents: BAS-Net Site Contacts will be responsible for advising their staff about BAS-Net security protocols as per the Agency Partner Agreement. Following a security incident, the BAS-Net Staff will also provide follow-up training to the organization staff – especially when new protocols have been recommended.

On-Going Review of Security Measures: The BAS-Net Administrator and BAS-Net Advisory Committee will be responsible for providing on-going monitoring of agency compliance with BAS-Net Policies and Procedures. This monitoring will include review of security policy and procedures and will occur on an annual basis.

System Access

Policy:	Participating agencies will apply the system and report access conventions set forth in the Standard Operating Procedures Manual. Agencies will manage the proper designation of user accounts to enforce aforementioned information security protocols.
----------------	--

System Access: Access to BAS-Net will be controlled based on need. Need exists only for those 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.

Access Levels: User accounts will be created and deleted by the BAS-Net Site Contact under the authorization of the agency's Executive Director. User access levels will be directly related to the user's job responsibilities and approved need for access to BAS-Net. The BAS-Net Administrator will issue a username and password for the BAS-Net Site Contact who will then disseminate usernames and passwords for agency users.

Below is a list of "Access Levels" and chart of activity designations within the BAS-Net system.

Resource Specialist I	Under this access level, a user may access only the ResourcePoint module. Users may search the database of area agencies and programs and view the agency or program detail screens. Access to client or service records and other modules and screens is not given. A resource specialist cannot add, modify or delete data.
Resource Specialist II	In addition to the access listed above, a Resource Specialist II is an agency-level "Information & Referral Specialist" who may update their own agency and program information.
Resource Specialist III	In addition to the access listed above, a Resource Specialist III may edit the system-wide news feature of BAS-Net.
Volunteer	Under this access level, a user may access ResourcePoint, and have limited access to ClientPoint, and to service records. A volunteer may view or edit basic demographic information about clients (the profile screen), but is restricted from all other screens in ClientPoint.

	A volunteer may also enter new clients, make referrals, or check-in/out a client from a shelter/facility. A volunteer does not have access to the "Services Provided" tab in BAS-Net. This access level is designed to allow a volunteer to perform basic intake steps with a new client and then refer the client to an agency staff or case manager.
Agency Staff	Under this access level, a user may access ResourcePoint, and have full access to service records, but only limited access to ClientPoint. Agency staff may access most functions in ServicePoint, however, they may only access basic demographic data on clients (profile screen). All other screens are restricted including Reports. Agency Staff can add news items to the NewsFlash feature of ServicePoint.
Case Manager I	Under this access level, a user may access all BAS-Net screens and modules except "Administration." A Case Manager I may access all screens within ClientPoint except, for confidentiality reasons, the medical screen. They also may access Reports.
Case Manager II	In addition to the access listed above, a Case Manager II may access all screens within ClientPoint, including the medical screen and Reports.
Agency Administrator	Under this access level, a user may access all ServicePoint screens and modules. This level may add/remove users and edit agency and program data for his/her agency.
Executive Director	Same access rights as Agency Administrator, but ranked above Agency Administrator.
System Operator	Under this access level, a user may just access "Administration." The system operator can setup new agencies, add new users, reset passwords, and access other system-level options. The system operator may order additional user licenses and modify the allocation of licenses. They maintain the system, but may not access any client or service records.
System Administrator I	Same access rights to client information as Agency Administrator, but excludes shadow mode. Full access to administrative functions.
System Administrator II	No restrictions. Full access to BAS-Net.

	Resource Specialist I	Resource Specialist II	Resource Specialist III	Volunteer	Agency Staff	Case Managers I & II	Agency Administrator	Executive Director	System Operators	System Administrator I	System Administrator II
ClientPoint											
Profile				X	X	X	X	X		X	X
Assessments						X	X	X		X	X
Case Notes						X	X	X		X	X
Case Plans						X	X	X		X	X
Service Records				X	X	X	X	X		X	X
ServicePoint											
Referrals				X	X	X	X	X		X	X
Services Provided					X	X	X	X		X	X
ResourcePoint	X	X	X	X	X	X	X	X	X	X	X
ShelterPoint				X	X	X	X	X		X	X
Reports											
<i>Audit Reports</i>											
Client/Service Information											X
User Information			X				X	X	X	X	X
Client/Service Access Information											X
<i>Provider Reports</i>											
Client Served						X	X	X		X	X
Daily Bed Report			X			X	X	X		X	X
HUD 40118 APR						X	X	X		X	X
Outstanding Referrals			X			X	X	X		X	X
Service Transaction						X	X	X		X	X
Needs Report						X	X	X		X	X
Report Writer						X	X	X		X	X
Administration											
Add/Edit Users							X	X	X	X	X
Reset Passwords							X	X	X	X	X
Add Provider			X						X	X	X
Edit Provider		#	X				#	#	X	X	X
Delete Provider		%	X				%	%	X	X	X
Agency News		X	X		X	X	X	X	X	X	X
System Wide News			X						X	X	X
Picklist Data									X	X	X
Licenses									X	X	X
Assessment Admin									X	X	X
Shadow Mode											X
System Preferences											X

X: Users have access to this section of ServicePoint.

%: Users can neither delete the provider they belong to, nor any of their parent providers.

#: Users cannot edit their parent provider, they may edit their provider or child providers only.

Passwords: Passwords are automatically generated by the BAS-Net system when a new user is created. BAS-Net Site Contacts will communicate the system-generated password to each respective agency user.

Each user will be required to change the password the first time they log onto the BAS-Net system. The password is alphanumeric and case sensitive. It must be between 8 and 16 characters and contain at least 2 numbers. Passwords are the individual's responsibility and users cannot share passwords under any circumstances. Passwords should not be easily guessed or found in any dictionary. They should be securely stored and inaccessible to other persons.

Passwords expire every 45 days. A password cannot be re-used until one entirely different password selection has expired.

User Termination or Extended Leave from Employment: The BAS-Net Site Contact should terminate the rights of a user immediately upon suspension or 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 BAS-Net Site Contact is responsible for removing users from the BAS-Net system. The BAS-Net Site Contact should also review the agency access list and signed agreements on a quarterly basis to ensure that records are up-to-date. The BAS-Net Site Contact must provide information about changes to the BAS-Net Administrator.

Sharing Data between Agencies: Agencies are restricted from viewing each other's client data unless specific sharing agreements have been negotiated. Clients must also grant permission to share information with a specified agency. Users will only be able to view the data entered by users of their own agency unless agreements are in place.

Report Access and Transport: Select BAS-Net users will have access to agency-level BAS-Net data in the form of reports and client case files. Access to this information is based on User Level and is determined based on need and authorized by the Agency Executive Director. Reasonable care should be taken when reviewing BAS-Net materials to ensure information is secure. Also See: Data Collection, Types, and Usage.

- Media and documents containing client-identified data should not be shared with any agency other than the owner of the data (and their partners) for any reason. An inter-agency sharing agreement and client consent must be secured before the agency shares information with another member of the system. Copies of the Interagency Data Sharing Agreement and the Client Consent and Release of Information Authorization forms can be found in the Supporting Documents section of this manual and on the HAWNY website.
- Printed versions of confidential data should not be copied or left unattended and open to unauthorized access. HMIS information in hardcopy format should be stored or disposed of properly.

- Authorized employees, using methods deemed appropriate by the participating agency, may transport BAS-Net data which meets approved security standards. However, a record of the transport – including information about the nature and type of information - must be maintained as well as a notification of information return.
- All client records containing identifying information that are stored within the Participating Agency's local computers are the responsibility of the participating agency.
- Media containing HMIS data that is released and/or disposed of by the participating agency should first be processed to destroy any data residing on that media. Degaussing, shredding and overwriting are acceptable methods of destroying data.

System Monitoring: The Site Contact will be responsible for monitoring all user access within their agency. Any violations or exceptions should be documented and forwarded to the BAS-Net Administrator immediately.

All suspected data, system security, and/or confidentiality violations will incur immediate user suspension from the BAS-Net system until the situation is effectively resolved. Serious or repeated violation by users of the system may result in the suspension or revocation of an agency's access to BAS-Net.

Any user found to be in violation of data, system security, and/or confidentiality protocols will be sanctioned accordingly. Recommended sanctions may include but, are not limited to, a formal letter of reprimand, suspension of system privileges, revocation of system privileges, termination of employment, 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 with input from the BAS-Net Advisory Committee. If an agency is found to be in violation, the sanction will be imposed by the BAS-Net Advisory Committee.

Agency Readiness Assessment and Training

Policy: Participating Agencies must complete the following Agency Readiness Assessment Procedure and Training before receiving a User Name and Password for the live BAS-Net site.

Partner Agreement: The BAS-Net Administrator will meet with the Executive Director or designee of a potential participating agency. The BAS-Net Administrator will provide information and answer questions about the BAS-Net system. The Executive Director or designee will review and sign the Agency Partner Agreement form. A copy of the Agency Partner Agreement is found in the Supporting Documents section of this manual and on the HAWNY website. These documents will be renewed on an “as needed” basis.

Identify Desire for Inter-Agency Data Sharing: In addition to the partner agreement, participating agencies may be interested in sharing data with another member of the BAS-Net system. In order to accomplish this, the Executive Directors from each of these agencies must sign an Inter-Agency Data Sharing Agreement. The BAS-Net staff will be available to facilitate dialogue between agencies, as needed. These documents will be renewed on an “as needed” basis.

Identify BAS-Net Site Contact: The Executive Director of the participating agency will select an individual as the designated BAS-Net Site Contact. The BAS-Net Site Contact will be the primary contact related to the system.

Identify Staff Participants: The Executive Director will work with the BAS-Net Site Contact to identify agency staff that will have access to BAS-Net and the level of access needed for each user. A User License Request will be completed for each user and submitted to the BAS-Net Administrator. Note: The grant provides three (3) user licenses at no cost. Additional licenses are to be purchased by the individual agency.

Evaluate Agency Hardware: The BAS-Net Administrator and/or BAS-Net Support Specialist will meet with the Site Contact to evaluate the hardware and Internet capacity of the site. Participating agencies will receive DSL service and one (1) computer and may utilize their own equipment to access the system. Agencies agree to maintain the integrity of the initial setup provided by HAWNY. If the agency terminates participation in BAS-Net, all hardware must be returned to HAWNY.

Evaluate Assessment and Report Customization Needs: The BAS-Net Administrator will meet with the Site Contact 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 required. Site Contacts may customize BAS-Net as needed, with the support of BAS-Net staff.

Evaluate Training Needs for Staff: The BAS-Net Administrator will meet with the Site Contact to determine the overall computer awareness and training needs of agency staff persons. All users should be familiar with Microsoft Windows applications and basic mouse skills before attending the Data Entry training.

Data Entry Training: The BAS-Net Administrator will set up training dates with the Site Contact for staff Data Entry training. All staff training will take place on a training web site and no actual data will be entered. A temporary training user name and password will be assigned to each user. The BAS-Net Administrator and Site Contact will also discuss any agency-specific policies and processes with agency staff at this time.

Standard Report Training: The BAS-Net Administrator will set up Agency Report training for staff that will have access to this feature. The main focus of this session will be on how to create standard HUD-required reports as well as basic queries.

Practice Entry: 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 Site Contact will evaluate additional training needs at this time based on issues that arise.

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

BAS-Net Site Contact Readiness: The BAS-Net Administrator will schedule a final meeting and training evaluation for agency staff. If the Site Contact and BAS-Net Administrator agree that the agency staff is ready, user IDs and Passwords will be generated by the BAS-Net Administrator and given to each agency user. The Site Contact will receive additional training to 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 BAS-Net Administrator.

Agency Data Collection Begins: The BAS-Net Administrator or Support Specialist will be available on-site for the first few hours of data collection to address any questions.

Reassessment and Monitoring: The BAS-Net Administrator will provide on-going trainings to address any agency staff turnover issues, or additional training and support that may be needed. It is the responsibility of the Site Contact to communicate with the BAS-Net Administrator when additional agency training is needed. All initial training and user creation should be done by the BAS-Net Administrator.

On-Going Training: Performance will be tracked by the BAS-Net Site Contact and/or Administrator and shared during user group meetings to determine further training needs and adjustments to the BAS-Net system, policies, and/or procedures. Each Site Contact should designate a representative to attend regular user group meetings.

Data Usage: Once live data entry has been integrated into the agency's daily operation for at least two months, participating organizations can begin using the information for internal evaluation and reporting requirements.

Inter-Agency Data Sharing

Policy: Personally-identifying data entered into BAS-Net will only be accessible to the agency that entered the client's data and will be initiated with a "Closed Security" status unless an Inter-Agency Data Sharing Agreement is put into place.

Agencies interested in sharing client data through the BAS-Net system must complete an Inter-Agency Data Sharing Agreement and must have necessary client consent. Copies of the Inter-Agency Data Sharing Agreement and Client Consent and Release of Information Authorization are located in the Supporting Documents section of this manual and on the HAWNY website.

Participating agencies who wish to share client data must contact the BAS-Net Administrator, schedule additional training, and complete all required consent forms before a change will be made to the client's on-line profile. BAS-Net staff is also available to facilitate dialogue and to discuss the pros and cons of data sharing between agencies, as needed.

As part of the agreement process, participating agencies will specify which data sections will be shared with the other identified agencies. In addition, clients have the option to specify what personal information they will share and with whom.

A client has the right to revoke consent for data sharing at any time.

When a client makes such a request, the agency staff person should ask the client to sign a Revocation of Consent form (available on the HAWNY website) to be forwarded to the BAS-Net Site Contact and immediately close or "re-lock" the client's record. To re-lock the record, simply click on each of the green security locks found on the client's profile and select the "closed" option.

In instances where the client will not or is unable to complete the Revocation of Consent form, the staff person should immediately close or "re-lock" the record and complete the bottom section of the Revocation of Consent form (available on the HAWNY website) stating that the client orally made the closure request and forward it to the BAS-Net Site Contact. To re-lock the record, simply click on each of the green security locks found on the client's profile and select the "closed" option.

Using the completed Revocation of Consent form, the BAS-Net Site Contact will ensure that the client's record was properly closed. This policy will be reviewed with staff periodically.

In the event that a client would like to "re-open" their file to sharing, staff members should follow standard consent procedures including written and electronic documentation of the decision.

Client Informed Consent and Release of Information

Policy: Participating agencies shall adhere to relevant federal and state confidentiality regulations and laws and agency policies that protect client records and only release client records with written consent by the client. A client must explicitly give permission for personal data to be shared with other agencies in BAS-Net. For minors, a parent or guardian must also give permission for their child's data to be shared.

Participating agencies are required to inform clients about the use of BAS-Net and to gain their consent prior to entering data into the computerized system. In addition, the agency must agree not to release any confidential information received via BAS-Net to any organization or individual without proper written consent.

Consumer Notice: All participating agencies will post a Consumer Notice at the point of data collection to inform clients of their intent to collect and enter data into the Buffalo Area Services Network (BAS-Net) Homeless Management Information System. A copy of the Consumer Notice is included in the Supporting Documents section of this manual and on the HAWNY website. The notice should be made available to clients upon request.

Privacy Notice: A notice detailing all privacy protections should be made available to clients upon request. A copy of the Privacy Protection Notice is included in the Supporting Documents section of this manual and on the HAWNY website.

Oral Informed Consent: Upon entry into a housing or service location, all clients will be provided an oral explanation that their information may be entered into a computerized record-keeping system with client consent. The partner agency will provide an explanation of both the BAS-Net project and the terms of consent. The agency is responsible for ensuring that this procedure takes place at the initial contact for every client. In instances where the client does not speak English or has difficulty understanding, it is expected that the agency will locate an appropriate and qualified interpreter.

The agency must share the following information:

What BAS-Net is

- An Internet-based information system that homeless services agencies use to capture information about the persons they serve.

Why the Agency Uses It

- To understand their client's needs
- To help the programs plan to have appropriate resources for their clients
- To inform public policy in an attempt to end homelessness

Security

- Only staff who work directly with clients or who have administrative responsibilities can look at, enter, or edit client records.

Privacy Protection

- Information that is transferred over the web is through a secure connection.
- No client information will be released to another agency without written consent.
- Client has the right to not answer a question, unless admission to the program requires it.
- Client has the right to know who has added to, deleted, or edited their record.

Benefits for Clients

- Case manager can tell clients about services available on-site or by referral.
- Case manager and client can use information to assist in obtaining resources.

Client consent to collect information and maintain confidentiality within the participating agency in a closed status will be assumed. All participating agency profiles will be initiated with a closed security status within ServicePoint.

Following initial intake (preferably during the first visit with a case manager), agency staff member will inquire if client is willing to have his or her information shared with other providers which are part of the BAS-Net system.

Written Informed Consent: Each client whose record is being shared electronically with a partner agency must agree via a signed Client Consent and Release of Information Authorization. A copy of the Client Consent and Release of Information Authorization form is available in the Supporting Documents section of this manual and on the HAWNY website. The client must specify what information can be shared and with whom it can be shared.

Such information should be documented in two ways:

- Paper Release of Information (ROI): Clients will specify what information can be shared and with whom on the Client Consent and Release of Information form. The release must be kept on file at the agency. At minimum, one paper copy of a release of information is required per agency and will cover all programs within an agency (unless agency policy differs). Clients should be given a copy of the paper release form for their information if requested.
- Software Release of Information (ROI): Client consent to the release of information must be attached to the client profile in the ServicePoint software. The ROI must be established prior to completing any assessment information in each program the client enters. The length of the ROI is one year, unless agency policy specifies otherwise.

NOTE: A CLIENT MAY NOT BE REFUSED SERVICES OF ANY KIND IF THEY DECLINE TO HAVE THE AGENCY SHARE THEIR INFORMATION THROUGH THE BAS-NET SYSTEM.

Entering Consent into BAS-Net: In the ServicePoint system, it is necessary to indicate that a release was granted in all cases.

- *If a client permits open sharing of his or her records or agrees to the default settings of the agency and signs a release to that effect, the agency user should indicate that a release was granted and that there is a “Signed Statement from the Client.” The agency will need to open each assessment so that outside agencies can view the information.*
- *When a client permits specified sharing of his or her records, the agency user would indicate that a release was granted and that there is a “Signed Statement from the Client.” In order to open specific client’s records to outside agencies while still keeping the information available within the agency requires either of the following steps:*
 - *If the client record has just been created, then go to the security lock in the right-hand corner of the screen in the orange bar and click the client’s record to open specified areas. Then check each of your programs in the possible exceptions to ensure that each will still have access to the data*
 - *If the client record is already in the system but the client now wants future information open, then go into each individual assessment and click on the security lock and change the record to open for each specified item. Then check each of your programs in the possible exceptions to ensure that each will still have access to the data.*
- *When a client does not permit any sharing of his or her information outside the agency, the user would indicate that a release was granted and that the type of release is “None.” The client’s records are already closed to outside agencies while the information is available within the agency:*
 - *If the client record has just been created, check each of your programs in the possible exceptions to ensure that each will still have access to the data*
 - *If the client record is already in the system but the client now wants future information closed, check each of your programs in the possible exceptions to ensure that each will still have access to the data.*
- *If a client calls a central point of intake and agrees to release the information to the referring agencies, the user would indicate that a release was granted and that there*

was Verbal Consent. The program profile would be set-up such that the release only allowed information to flow to the other programs in the agency or to those programs for which the central point of intake has an agreement.

Revocation of Consent: A client has the right to revoke consent for data sharing at any time. When a client makes such a request, the agency staff person should ask the client to sign a Revocation of Consent form (available on the HAWNY website) to be forwarded to the BAS-Net Site Contact and immediately close or “re-lock” the client’s record. To re-lock the record, simply click on each of the green security locks found on the client’s profile and select the “closed” option.

In instances where the client will not or is unable to complete the Revocation of Consent form, the staff person should immediately close or “re-lock” the record and complete the bottom section of the Revocation of Consent form (available on the HAWNY website) stating that the client orally made the closure request and forward it to the BAS-Net Site Contact. To re-lock the record, simply click on each of the green security locks found on the client’s profile and select the “closed” option.

Using the completed Revocation of Consent form, the BAS-Net Site Contact will ensure that the client’s record was properly closed. This policy will be reviewed with staff periodically.

In the event that a client would like to “re-open” their file to sharing, staff members should follow standard consent procedures including written and electronic documentation of the decision.

Unnecessary Solicitation: The Participating Agency must not solicit or input information from clients unless it is clearly in the client’s best interest and is essential to provide services or to conduct research/program evaluation.

Server Access: Participating agencies must understand that Bowman Internet Systems will maintain the server that will contains all client information. All client-identified data is inaccessible to unauthorized users.

Data Collection, Types, and Usage

Policy:	Participating agencies that gather client data through BAS-Net agree to collect required data elements derived from HUD Data and Technical Standards and recommendations made by the BAS-Net Advisory Committee. These data elements will ensure that the community has necessary information to measure system usage and to draw inferences about the homeless population and their needs. The nature of BAS-Net data will be assessed and appropriate controls implemented to ensure that all data is handled according to the following procedures.
----------------	--

Mandatory Data Collection: Each participating agency is responsible for ensuring that all clients are asked a mandatory set of questions for use in aggregated analyses. These questions are included in the various assessments located within the ServicePoint system. Within each assessment the mandatory data elements will be displayed in RED text or will otherwise indicate that the field is required. Partner agencies agree to enter this information into BAS-Net.

Assessments: The BAS-Net Administrator will work with the Site Contact to identify the most appropriate assessments for individual partner agencies. In doing so, the BAS-Net Administrator will ensure that each program is completing the required HUD universal and program-specific data elements as part of their regular client assessments.

Administration of Data: BAS-Net and approved participating agency staff members will administer data by adhering to a set of controls required for enforcing and maintaining security standards. Appropriate procedures for transmission and storage are included below.

Data Types: There are two mutually exclusive types of data available in BAS-Net.

Open Data: Unrestricted information that contains no data elements that are or could be used as personal identifiers.

Confidential Data: Information that can be used to identify a client whose information is contained within the BAS-Net system. Examples include: Social Security Number, name, address, or any other information that can be used to identify a client. Any material that includes any confidential information shall be considered confidential data.

Procedures for Transmission and Storage of Open and Confidential Data: All data must be classified open or confidential. Failure to handle data properly is a violation.

Open Data is typically subject to further classification and scrutiny depending on the intent for the data and its audience. Unless this data is to be used as “Public Data,” then it should be handled discretely.

Confidential Data may be used for internal analysis or in the preliminary process of creating open data. BAS-Net Administrators may also work with confidential data in the process of assisting partner agencies or correcting system errors.

In keeping with HUD's Data and Technical standards and as outlines in the BAS-Net Partner Agreement, hard copies shall be:

- Stored in a secure environment generally inaccessible to other staff or the public
- Not left out in the open or unattended; and
- Properly disposed when no longer needed following agency policy (i.e., shredded).

In keeping with HUD's Data and Technical standards and as outlines in the BAS-Net Partner Agreement, electronic copies shall be:

- Stored only where approved staff members can access the data;
- Stored where a password is required to access data if on shared server space; and
- Kept under the staff members physical control (e.g., CD-ROM, personal computer)
- Properly disposed when no longer needed following agency policy (i.e., deleted).

Data Usage: There are three mutually-exclusive types of usage for BAS-Net data.

Public Usage: Information from BAS-Net that is shared with the general public in written, electronic or verbal format

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

Restricted Usage: Information that has been created or accessed primarily for administrative purposes. This data may or may not eventually be made public.

Procedures for Handling Public, Internal, or Restricted Usage: All data usage must be classified public, internal, or restricted. Failure to handle data properly is a violation.

Public Usage: Security controls are not required but data must not include any client identifiers such that an individual could be identified even through inference. The data shall reasonably reflect the elements from which it was derived and shall identify constraints or inferences related to its use or generalizability.

Internal Usage: Data is accessible only to internal employees. No auditing is required. No special requirements around destruction of these data are required. These data must be stored out of site and can be transmitted via internal or first-class mail.

Restricted Usage: Data is available only on a need-to-know access basis. Requires auditing of access and must be stored in a secure location. There are not special requirements around destruction of these data. If mailed internally or externally, it must be labeled confidential.

Data Quality and Control

Policy: BAS-Net Staff and the BAS-Net Advisory Board will occasionally monitor data collection activities and review participating agency compliance. BAS-Net partner agencies are responsible for the overall quality, accuracy, and completeness of data entered by their staff members. In addition, the nature of BAS-Net data will be assessed and appropriate controls implemented to ensure that information is handled properly.

Minimum Participation: Standards for minimum partner agency participation will be established by BAS-Net Advisory Board. The BAS-Net Administrator will run system-wide reports to assess the level and quality of participation by partner agencies. Results from these reviews will be shared with the BAS-Net Site Contact at each agency.

Data Integrity: All BAS-Net users will be responsible for the accuracy of their data entry. In order to test the integrity of the data contained in the system, the BAS-Net Administrator will perform regular data integrity checks. Any patterns of error will be reported to the BAS-Net Site Contact. When patterns of error have been discovered, agency users will be required to correct data entry techniques. These corrections will be reviewed to assess compliance.

Data Integrity Expectations: It is expected that participating agencies will provide the following levels of accuracy and timeliness:

- All names and Social Security Numbers will be accurate (in as much as possible);
- Data will be entered in a consistent manner; and
- Agencies will strive for real-time, or close to real-time, data entry.

Data Access: As per executed BAS-Net Agreement, approved staff members from participating agencies will have access to individual and aggregated 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 Inter-Agency Data Sharing Agreement and through explicit client consent.

Data Retrieval: Participating agencies will create and run their own agency-level reports. The BAS-Net Site Contact will be trained in reporting by the BAS-Net Administrator and will serve as the primary agency resource for report creation. Other agency staff members may be able to generate and print reports depending upon their access level. See: Data Collection, Types, and Usage for more information.

Public Access to Data: The BAS-Net Administrator, on behalf of the BAS-Net Advisory Committee, will address all external requests for data from non-participating entities. As part of the BAS-Net Administrator's regular employment functions, periodic public reports about homelessness in Buffalo and Erie County will be generated and shared. No confidential client data will be included in these reports.

Data Ownership

Policy: The BAS-Net Advisory Committee will establish data ownership for the local HMIS. Ownership is outlined in this Standard Operating Procedures Manual.

Participating agencies are the owners of all client data collected and stored within the BAS-Net system. This data is protected and secured by the policies, technologies, and security protocols held in place.

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 BAS-Net.

Grievances

Policy:	The BAS-Net Advisory Committee will monitor and, if necessary, address Client and Agency grievances related to the operation of the local HMIS. BAS-Net Staff grievances will be addressed by the BAS-Net Administrator and/or the Executive Director of the Homeless Alliance of Western New York.
----------------	---

Client Grievances: Clients with a BAS-Net-related grievance should first identify their concerns to their regular staff member. Upon learning of the grievance, the staff member is required to communicate the concern to their BAS-Net Site Contact for review and possible resolution. The client should also be given the “BAS-Net Grievance Flow Chart” (available on HAWNY website) which details procedures and contact information.

Each participating agency is responsible for addressing client questions and complaints regarding the BAS-Net system to the best of their ability and in accordance with their agency grievance policies. Possible actions may include further investigation of incidents, clarification or review of policies, or sanctioning of users (if users are found to have violated standards set forth in BAS-Net agreements or this Standard Operating Procedures Manual). Participating agencies are also obligated to report all BAS-Net-related client grievances to the BAS-Net Administrator using the BAS-Net Grievance Form (available on the HAWNY Website).

If a client grievance is not satisfactorily resolved at the agency level, the client may contact the BAS-Net Administrator. The BAS-Net Administrator will attempt to resolve the issue. If necessary, the Administrator will present the problem to the BAS-Net Advisory Committee at their next meeting. The BAS-Net Advisory Committee will be given an opportunity to review the details and facts of a situation and will present recommendations towards resolution to the HAWNY Board of Directors. The HAWNY Board of Directors will have final decision-making authority.

Agency Grievances: Any problems related to the operation or policies of BAS-Net or its participating agencies should be directed to the BAS-Net Administrator. S/he is responsible for addressing agency-level questions and complaints regarding the BAS-Net system to the best of their ability. Possible actions may include further investigation of incidents, clarification or review of policies, or sanctioning of participating agencies. The BAS-Net Administrator is also obligated to report all BAS-Net-related agency grievances to the BAS-Net Advisory Committee using the BAS-Net Grievance Form (available on the HAWNY Website).

If an agency issue is not satisfactorily resolved by the BAS-Net Administrator, the agency may bring the issue to the BAS-Net Advisory Committee. The BAS-Net Advisory Committee will provide information related to the details and facts of a situation to the HAWNY Board of Directors as well as recommendations towards resolution. The HAWNY Board of Directors will have final decision-making authority.

Reporting Client and Agency Grievances: The BAS-Net Administrator will be responsible for providing a summary of all grievances and their resolutions to the BAS-Net Advisory Committee on a monthly basis.

BAS-Net Staff Grievances: Any problems with the BAS-Net Support Staff should first be reported to the BAS-Net Administrator. The BAS-Net Administrator will seek to resolve the issue and will identify staffing concerns to the Executive Director of the Homeless Alliance of Western New York as appropriate.

Any grievances against the BAS-Net Administrator should be made directly to the Executive Director of the Homeless Alliance of Western New York for resolution.

Termination of Participation

Policy: The BAS-Net Advisory Committee will establish requirements related to termination of agency participation in the local HMIS. All requirements for termination are outlined in this Standard Operating Procedures Manual.

Voluntary Termination: To discontinue participation in BAS-Net, an agency must submit written notice to the BAS-Net Administrator. Upon receipt of this written notice, all licenses assigned to that agency will be discontinued by 5pm on the last day of that month.

In addition:

- All BAS-Net equipment must be returned to HAWNY by 5pm on the last day of the month.
- Any costs associated with transferring/exporting data out of the BAS-Net will be the responsibility of the terminating agency.
- Any additional licenses or service contracts that have been purchased by the agency outside of the HAWNY-provided services may cause the agency to incur an early withdrawal fee.

Involuntary Termination: In the event that the BAS-Net Advisory Committee decides to terminate an agency from the BAS-Net system, the committee will submit a written notice to the agency's Executive Director identifying a termination date. On that termination date, all licenses assigned to that agency will be discontinued at 5pm, unless an effective date was otherwise established.

In addition:

- All BAS-Net equipment must be returned to HAWNY within one week of the termination date.
- Any costs associated with transferring/exporting data out of the BAS-Net will be the responsibility of the terminated agency.
- Any additional licenses or service contracts that have been purchased by the agency outside of the HAWNY-provided services may cause the agency to incur an early withdrawal fee.

Program Termination: In the event that the BAS-Net Project ceases to exist, Partner Agencies will be notified and provided reasonable time to access and save Client data on those served by the agency, as well as statistical and frequency data from the entire

system. Thereafter, the information collected by the centralized server will be purged or appropriately stored.

HAWNY Termination: In the event that HAWNY ceases to exist, the custodianship of the data within BAS-Net will be transferred by HAWNY to another organization for continuing administration, and all BAS-Net Partner Agencies will be informed in a timely manner.

Use of Unnamed Client Feature

Policy:	Use of the Unnamed Client Feature is available through Service Point to authorized staff on a limited basis. This feature may only be used in domestic violence situations or when the client does not authorize the agency staff to input personally identifiable information into the BAS-Net System. When using this feature, only anonymous information will be shared with the Homeless Alliance.
Use of the Anonymous Client Feature is not authorized at any time.	

Bowman Internet Systems has developed a client entry option that allows the input of client information without saving the client's name into the database. It uses an algorithm similar to the one used for "Named Clients" and provides a more accurate unduplicated client count than using the "Anonymous Client" record. Although this feature does not use the Social Security Number to create the identifier, it will allow organizations to include this information after initial intake.

Authorization of the use of the Unnamed Client Feature is restricted to persons with Agency Administrator (or Executive Director) level access in the BAS-Net system and must only be used for clients who are unwilling to disclose their personally identifying information (i.e., name) to the Homeless Alliance of Western New York because of domestic violence or other special concerns.

To use the Unnamed Client Feature, Agency Administrators must first contact the BAS-Net System Administrator in order to have their System Preferences modified. Once changes have been made, the Agency Administrator will be able to modify the specific user profiles to enable the "Manage Unnamed Clients" feature by checking the appropriate box. Modifications can be made using the Admin - Users screen.

Note: Providers should be aware that once the Agency Administrator (or Executive Director) enables "Manage Unnamed Clients" feature, the user will be unable to search for Named Clients until the Unnamed Client feature is disabled and the user's profile is returned to its original state.

When enabled, users will observe that the first and last name of the client do not appear in the profile. Instead, "Unnamed" appears in the first name field and the client number appears in the last name field. Users will not be able to modify these fields. The data entered for Date of Birth, Gender, and Race are retained within the system for the purposes of aggregate reporting. All other features and assessments are available.

Once the new Unnamed Client profile screen is closed, providers will be unable to acquire the client's id number through the system. Without the client's Unnamed Client id number, users will not be able to search for or locate a client previously entered into the system. Therefore, a protocol should be established by the agency to securely retain client id information. Providers should include the assigned code in the client record to ensure that they will be able to access the file. **It is not possible to share the records of unnamed clients with other BAS-Net participating organizations.**

IV. Supporting Documents

Agency Partner Agreement
Inter-Agency Data Sharing Agreement
User Policy, Responsibility Statement, and Code of Ethics
Client Consent and Release of Information Authorization
Client Consent and Release of Information Authorization (HIPPA)
Consumer Notice
Privacy Protection Notice
User License Request
Grievance Form
Security Incident Report
Revocation of Consent Form
Glossary of Terms

AGENCY PARTNER AGREEMENT
For Buffalo Area Services Network (BAS-Net)

This agreement is entered into on _____ (dd/mm/yyyy) between the Homeless Alliance of Western New York (System Administrator), hereafter known as "HAWNY," and _____, hereafter the "Agency," regarding access and use of the Buffalo Area Services Network Homeless Management Information System, hereafter known as "BAS-Net."

I. Introduction

BAS-Net, an Internet-based management information system, allows authorized personnel at homeless housing and service provider agencies throughout the Buffalo and Erie County area to enter, track, and report on information concerning their own Clients and to share information, subject to Client consent and appropriate inter-agency agreements.

BAS-Net goals are to:

- provide a user-friendly and high-quality automated records system that expedites Client intake procedures, improves referral accuracy, and supports the collection of quality information that can be used for program improvement and service-planning;
- improve care coordination for homeless persons in Buffalo and Erie County; and
- meet reporting requirements as established by the U.S. Department of Housing and Urban Development and other funders as needed.

In compliance with all federal requirements regarding Client/consumer confidentiality and data security, BAS-Net is designed to collect and deliver timely, credible, quality data about services and homeless persons or persons at risk for being homeless.

BAS-Net utilizes the ServicePoint Client Information Management System developed by Bowman Internet Systems. ServicePoint is a Client information system that provides a standardized assessment of consumer need, creates individualized service plans, and records the use of housing and services. Communities can use this information to better understand the use of services, identify gaps in the local service continuum, and develop outcome measurements.

Parties to this Agreement are HAWNY, the System Administrator, who is the coordinating agency of BAS-Net; and the "Agency" who is named above in the Agreement.

References in this Agreement to "Partner Agency" describe all other agencies entering into an Agency Partner Agreement. "Client" is a consumer of services.

Signatures of Executive Directors from HAWNY and the Agency indicate agreement with the terms set forth before an Agency ServicePoint account can be established.

II. HAWNY Responsibilities

1. HAWNY will provide the Agency 24-hour access to the BAS-Net data-gathering system, via Internet connection.
2. HAWNY will provide one (1) computer and three (3) user licenses to each BAS-Net Agency. Additional user licenses may be purchased by the Agency under separate contract.
3. Initial DSL Internet-connection and service, security locks, and anti-virus software and updates will be provided by HAWNY. The Initial grant is for three (3) years.
4. HAWNY will provide the Client Consent and Release of Information Authorization form (See: BAS-Net Standard Operating Procedures Manual).
5. HAWNY will provide both initial training and periodic updates to that training for core Agency Staff regarding the use of BAS-Net.
6. HAWNY will provide basic user support and technical assistance (i.e., general trouble-shooting and assistance with standard report generation) in accordance with procedures that will be periodically updated and published by HAWNY.
7. HAWNY will not publish reports on Client data that identify specific agencies or persons without prior agency (and where necessary, Client) permission. Public reports otherwise published will be limited to presentation of aggregated, or summary, data within BAS-Net.
8. HAWNY's publication practice will be governed by policies established by its Board and recommended by committees.

III. Privacy and Confidentiality

A. Protection of Client Privacy

1. The Agency that is considered a "covered entity" under the Health Insurance Portability and Accountability Act of 1996, 45 C.F.R., Parts 160 & 164, and corresponding regulations established by the U.S. Department of Health and Human Services is required to operate in accordance with HIPAA regulations.
2. The Agency not considered a "covered entity" under the Health Insurance Portability and Accountability Act of 1996, 45 C.F.R., Parts 160 & 164, and corresponding regulations established by the U.S. Department of Health and Human Services is required to operate in accordance with HMIS privacy and security rules.
3. The Agency will comply with all applicable federal and state laws regarding protection of Client privacy.
4. The Agency will comply with all policies and procedures established by HAWNY pertaining to protection of Client privacy.

B. Client Confidentiality

1. The Agency agrees to post a Consumer Notice at the point of data collection to inform clients of their intent to collect and enter data into the Buffalo Area Services Network (BAS-Net) Homeless Management Information System. Copies of the notice will be available to Clients upon request. (See: BAS-Net Standard Operating Procedures Manual).
2. The Agency will provide copies of the Privacy Protection Notice, detailing all privacy protections in place within the BAS-Net system, to any Client upon request. (See: BAS-Net Standard Operating Procedures Manual).
3. The Agency will provide an oral explanation of the BAS-Net system and arrange for an appropriate and qualified interpreter in the event that an individual has difficulty understanding.
4. The Agency will not solicit or enter information from Clients into BAS-Net unless it is essential to provide services.
5. The Agency will not divulge any confidential information received from BAS-Net to any organization or individual without signed written consent (Client Consent and Release of Information form) from the Client, unless otherwise permitted by applicable regulations or laws.
6. The Agency will ensure that all persons who are issued a User Identification and Password to the BAS-Net abide by this agreement, including all associated confidentiality provisions. The Agency will be responsible for oversight of its own related confidentiality requirements.
7. The Agency agrees that it will ensure that all persons issued a User ID and Password will complete a formal training provided by Bowman Internet Systems, HAWNY, or HAWNY-designated trainers on privacy and confidentiality policies and BAS-Net. Employees must demonstrate mastery of that information prior to activation of their User License.
8. The Agency agrees that those granted Agency Administrator system access must first become a BAS-Net Agency Administrator through training provided by Bowman Internet Systems, HAWNY, or HAWNY-designated trainers.
9. The Agency acknowledges that ensuring the confidentiality, security and privacy of any information downloaded from the system by the Agency is strictly the responsibility of the Agency.

C. Inter-Agency Data Sharing

1. The Agency acknowledges that forms provided by HAWNY regarding Client privacy and confidentiality are models which may require modifications in accordance with Agency-specific rules. Any modification to forms must be submitted in writing to HAWNY for review and approval by HAWNY.

2. The Agency acknowledges that Client consent is required before any basic identifying Client information is shared with other agencies in the system. The Agency will document Client consent on the BAS-Net Client Consent and Release of Information Authorization form (See: BAS-Net Standard Operating Procedures Manual).
3. If the Client has given approval through a completed BAS-Net Client Consent and Release of Information Authorization form, the Agency may elect to share information according to Inter-Agency Data Sharing Agreement that the Agency has negotiated with other partnering agencies in BAS-Net.
4. The Agency agrees to develop a plan for all routine sharing practices with partnering Agencies and document that plan through a fully executed Inter-Agency Data Sharing Agreement form (See: BAS-Net Standard Operating Procedures Manual).
5. The Agency will incorporate a BAS-Net release clause into its existing Agency Authorization for Release of Information Form(s) if the Agency intends to share restricted Client data within BAS-Net.
6. Restricted information, including progress notes and psychotherapy notes about the diagnosis, treatment, or referrals related to a mental health disorder, drug or alcohol disorder, HIV/AIDS, and domestic violence concerns shall not be shared with other participating Agencies without the Client's written consent as documented on the Agency-modified Authorization for Release form. Sharing of restricted information is not covered under the general BAS-Net Client Consent and Release of Information Authorization form. Sharing of restricted information must also be planned and documented through a fully executed Inter-Agency Data Sharing Agreement.
7. Agencies with whom information is shared are each responsible for obtaining appropriate Client consent(s) before allowing further sharing of Client records.
8. The Agency acknowledges that the Agency, itself, bears primary responsibility for oversight for all sharing of data it has collected via BAS-Net.
9. The Agency agrees to place all Client Consent and Release of Information Authorization forms related to BAS-Net in a file to be located at the Agency's business address and that such forms will be made available to HAWNY for periodic audits. The Agency will retain these BAS-Net-related forms for a period of 7 years, after which time the forms will be discarded in a manner that ensures Client confidentiality is not compromised.
10. The Agency acknowledges that Clients who choose not to authorize sharing of information shall not be denied services for which they would otherwise be eligible.

D. Custody of Data

1. The Agency understands that the Client data will be encrypted at the server level using encryption technology.
2. The Agency understands the file server, which will contain all Client information, including encrypted identifying Client information, will be located at Bowman Internet System, Inc. offices at 400 Travis Street, Suite 1900, Shreveport, LA 71101.
3. The Agency acknowledges, and HAWNY agrees, that the Agency retains ownership over all information it enters into BAS-Net.
4. If this Agreement is terminated, the Homeless Alliance of Western New York and remaining Partner Agencies shall maintain their right to the use of all Client data previously entered by the terminating Agency; this use is subject to any restrictions requested by the Client.
5. In the event that the BAS-Net Project ceases to exist, Partner Agencies will be notified and provided reasonable time to access and save Client data on those served by the agency, as well as statistical and frequency data from the entire system. Thereafter, the information collected by the centralized server will be purged or appropriately stored.
6. In the event that HAWNY ceases to exist, the custodianship of the data within BAS-Net will be transferred by HAWNY to another organization for continuing administration, and all BAS-Net Partner Agencies will be informed in a timely manner.

IV. Data Entry and Regular Use of BAS-Net

1. The Agency shall follow, comply with and enforce the User Policy, Responsibility Statement, & Code of Ethics form signed by Agency employees (See: BAS-Net Standard Operating Procedures Manual). The User Policy, Responsibility Statement & Code of Ethics form may be modified by HAWNY as needed for the purpose of the smooth and efficient operation of the BAS-Net system. HAWNY will announce approved modifications to the User Policy, Responsibility Statement & Code of Ethics form in a timely manner via Newsflash.
2. The Agency will not permit User IDs and Passwords to be shared among users.
3. The Agency will only enter into BAS-Net individuals that exist as Clients under the Agency's jurisdiction. The Agency shall not misrepresent its Client base in the BAS-Net system by entering known inaccurate information.

4. The Agency will not alter information that is entered into BAS-Net by another Agency with known inaccurate information (i.e. Agency will not purposefully enter inaccurate information to override information entered by another Agency).
5. The Agency will not knowingly enter inaccurate information into BAS-Net.
6. The Agency shall use Client information in the ServicePoint database, as provided to the Agency or Partner Agencies, to assist the Agency in providing adequate and appropriate services to the Client.
7. If a Client has previously given the Agency permission to share information with multiple agencies beyond basic identifying information and non-restricted service transactions, and then chooses to revoke that permission to one or more of these agencies, the Agency will contact its Partner Agency/Agencies and explain that, at the Client's request, portions of that Client record will no longer be shared. The Agency will then "lock" those portions of the record impacted by the revocation to the other agency or agencies.
8. If the Agency receives information that necessitates a Client's information be entirely removed from BAS-Net, the Agency will work with the Client to complete a brief statement, which will be sent to the BAS-Net Administrator for de-activation of the Client record.
9. The Agency will enter all required data elements as defined by HAWNY and the U.S. Department of Housing and Urban Development.
10. The Agency will enter data in a consistent manner, and will strive for real-time, or close to real-time, data entry.
11. The Agency will routinely review records it has entered into BAS-Net for completeness and data accuracy.
12. The Agency acknowledges that with a current standard BAS-Net Client Consent and Release of Information Authorization form on file, it can update, edit, and print out a Client's information. Once the form is expired, the Agency can no longer edit or print the record.
13. The Agency acknowledges that once that Client Consent and Release of Information Authorization form expires, any new information entered into the database will be closed to sharing. Information entered before the date of the expired release will continue to be available to the sharing partners.
14. The Agency acknowledges that a modified-Agency Authorization to Release Information form, with a BAS-Net clause, permits it to share restricted Client information with select agencies in compliance with the Agency's approved

Confidentiality Policies and Procedures.

15. The Agency will prohibit anyone with an Agency-assigned User ID and Password from entering offensive language, profanity, or discriminatory comments based on race, color, religion, national origin, ancestry, handicap, age, sex, and/or sexual orientation.
16. The Agency and its employees will utilize BAS-Net for business purposes only.
17. The Agency will keep updated virus protection software on Agency computers that access BAS-Net.
18. Transmission of material in violation of any United States Federal or State regulations is prohibited. This includes, but is not limited to, copyrighted material, material legally judged to be threatening or obscene, and material considered protected by trade secret.
19. The Agency will not use BAS-Net with intent to defraud the Federal, State, or local government, or an individual entity, or to conduct any illegal activity.
20. The Agency agrees that HAWNY may convene local or regional user meetings to discuss procedures, updates, policy and practice guidelines, data analysis, and software/ hardware upgrades. The Agency will designate at least one specific staff member to regularly attend user meetings.
21. The Agency will incorporate procedures for responding to Client concerns regarding use of BAS-Net into its existing Grievance Policy. While appeals to BAS-Net should not be considered part of the formal process, a copy of any HMIS-related grievance, and the Agency's response, must be submitted to the BAS-Net Administrator.
22. Notwithstanding any other provision of this Participation Agreement, the Agency agrees to abide by all policies and procedures relevant to the use of BAS-Net that HAWNY publishes from time to time.

V. Publication of Reports

1. The Agency agrees that it may only release aggregated, or summary, information generated by BAS-Net that is specific to its own services.
2. The Agency shall retain access to identifying and statistical data on the Clients it serves.
3. The Agency may make aggregated data available to other entities for funding or planning purposes pertaining to providing services to homeless persons.

However, such aggregate data should not directly identify individual Clients or agencies without expressed permission.

4. HAWNY will use only unidentified, aggregate BAS-Net data for homeless policy and planning decisions, in preparing federal, state, or local applications for homelessness funding, to demonstrate the need for and effectiveness of a program, and to obtain a view of program utilization.

VI. Database Integrity

1. The Agency will not share assigned User IDs and Passwords to access BAS-Net with any other organization, governmental entity, business, or individual.
2. The Agency will not intentionally cause corruption of BAS-Net in any manner. Any unauthorized access or unauthorized modification to computer system information, or interference with normal system operations, will result in immediate suspension of services, and, where appropriate, legal action against the offending entities.

VII. Hold Harmless

1. HAWNY makes no warranties, expressed or implied. The Agency, at all times, will indemnify and hold HAWNY harmless from any damages, liabilities, claims, and expenses that may be claimed against the Agency; or for injuries or damages to the Agency or another party arising from participation in the BAS-Net; or arising from any acts, omissions, neglect, or fault of the Agency or its agents, employees, licensees, or Clients; or arising from the Agency's failure to comply with laws, statutes, ordinances, or regulations applicable to it or the conduct of its business.
2. This Agency will hold HAWNY harmless for loss or damage resulting in the loss of data due to delays, non-deliveries, mis-deliveries, or service interruption caused by Bowman Information Systems, by the Agency's or other member agency's negligence or errors or omissions, as well as natural disasters, technological difficulties, and/ or acts of God.
3. HAWNY shall not be liable to the Agency for damages, losses, or injuries to the Agency or another party other than if such is the result of gross negligence or willful misconduct of HAWNY.
4. HAWNY agrees to hold the Agency harmless from any damages, liabilities, claims or expenses caused solely by the negligence or misconduct of HAWNY.
5. The Agency agrees to keep in force a comprehensive general liability insurance policy with combined single limit coverage of not less than one million dollars (\$1,000,000). Said insurance policy shall include coverage for theft or damage of the Agency's BAS-Net-related hardware and software, as well as coverage of Agency's indemnification obligations under this

agreement. The Agency shall list HAWNY as additionally insured in such coverage.

VIII. Terms and Conditions

1. The parties hereto agree that this agreement is the complete and exclusive statement of the agreement between parties and supersedes all prior proposals and understandings, oral and written, relating to the subject matter of this agreement.
2. The Agency shall not transfer or assign any rights or obligations under the Participation Agreement without the written consent of HAWNY.
3. This agreement shall remain in force until revoked in writing by either party, with 30 days advance written notice. The exception to this term is if allegations or actual incidences arise regarding possible or actual breaches of this agreement. Should such situations arise, HAWNY may immediately suspend access to BAS-Net until the allegations are resolved in order to protect the integrity of the system.
4. This agreement may be modified or amended by written agreement executed by both parties with 30 days advance written notice.

Signature of Executive Director

Date

AGENCY

FEIN

STREET ADDRESS

CITY

STATE

ZIP CODE

MAILING ADDRESS (IF DIFFERENT FROM ABOVE)

CITY

STATE

ZIP CODE

Signature of HAWNY Executive Director

Date

AGENCY

FEIN

STREET ADDRESS

CITY

STATE

ZIP CODE

MAILING ADDRESS (IF DIFFERENT FROM ABOVE)

CITY

STATE

ZIP CODE

INTER-AGENCY DATA SHARING AGREEMENT
For Buffalo Area Services Network (BAS-Net)

The Homeless Alliance of Western New York administers a computerized management information system that captures information about people experiencing homelessness, including their service needs. The system, known as BAS-Net, enables programs to electronically share information about Clients who have been entered into the system. Client-level information can only be shared between agencies that have established an Inter-Agency Sharing Agreement and have received written consent from particular Clients agreeing to share their personal information with another agency. The agency receiving written consent has the ability to “share” Client information electronically through the system with a collaborating agency.

This process can benefit Clients by eliminating duplicate intakes. Intake and exit interviews can be shared, with written consent, between _____ and _____ (NAMES OF COLLABORATING AGENCIES).

By establishing this agreement, the _____ (NAMES OF COLLABORATING AGENCIES) agree that within the confines of BAS-Net System:

- 1) System information in either paper or electronic form will never be shared outside of the originating agency without Client written consent.
- 2) Client-level information will only be shared electronically through the System with agencies the Client has authorized to see their information.
- 3) **Information that is shared with written consent will not be used to harm or deny any services to a Client.**
- 4) A violation of the above by any Agency employee will result in immediate disciplinary action by the Agency.
- 5) Information will be deleted from the system upon Client request.
- 6) Clients have the right to request information about who has viewed or updated their record in BAS-Net.
- 7) Agencies must comply with all applicable federal and state laws and regulations regarding privacy and confidentiality.

We at _____ (NAMES OF COLLABORATING AGENCIES) establish this Inter-Agency Sharing Agreement so that our agencies will have the ability to share Client-level information electronically through BAS-Net. This agreement does not pertain to Client-level information that has not been entered into the system. This electronic sharing capability only provides us with a tool to share Client-level information. This tool will only be used when a Client provides written consent to have his/her information shared.

_____ (NAMES OF COLLABORATING AGENCIES) also have an agreement with the Homeless Alliance of Western New York and have completed security procedures regarding the protection and sharing of Client data.

By signing this form, on behalf of our agencies, I authorize the Homeless Alliance of Western New York to allow us to share information between our agencies through BAS-Net. We agree to follow all of the above policies to share information between our collaborating agencies.

Agency 1

Agency 2

Printed Name of Executive Director

Printed Name of Executive Director

Signature of Executive Director

Signature of Executive Director

Date

Date

**USER POLICY, RESPONSIBILITY STATEMENT,
& CODE OF ETHICS**
For Buffalo Area Service Network (BAS-Net)

USER POLICY

Partner Agencies will share information for provision of services to homeless persons through a networked infrastructure that establishes electronic communication among the Partner Agencies.

Partner Agencies will at all times have rights to the data pertaining to their Clients that was created or entered by them in BAS-Net. Partner Agencies shall be bound by all restrictions imposed by Clients pertaining to the use of personal data that they do not formally release.

It is a Client's decision about which information, if any, entered into BAS-Net shall be shared and with which Partner Agencies. The BAS-Net Client Consent and Release of Information shall be signed if the Client agrees to share information with Partner Agencies.

Minimum data entry on each consenting Client will be:

- Completing the HUD 40118 Worksheet
- Each shelter bed reservation and use

Data necessary for the development of aggregate reports of homeless services, including services needed, services provided, referrals and Client goals and outcomes should be entered to the greatest extent possible.

BAS-Net is a tool to assist agencies in focusing services and locating alternative resources to help homeless persons. Therefore, agency staff should use the Client information in BAS-Net system to target services to the Client's needs.

USER RESPONSIBILITY

Your User ID and Password gives you access to BAS-Net. Initial each item below to indicate your understanding and acceptance of the proper use of your User ID and password. Failure to uphold the confidentiality standards set forth below is grounds for immediate termination from BAS-Net.

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

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

_____ I understand that the only individuals who can view information in BAS-Net are authorized users and the Clients to whom the information pertains.

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

_____ If I am logged into BAS-Net and must leave the work area where the computer is located, I **must log-off** of BAS-Net before leaving the work area.

_____ A computer that has BAS-Net “open and running” shall never be left unattended.

_____ Failure to log off BAS-Net appropriately may result in a breach in Client confidentiality and system security.

_____ Hard copies of BAS-Net information must be kept in a secure file.

_____ When hard copies of BAS-Net information are no longer needed, they must be properly destroyed to maintain confidentiality.

_____ If I notice or suspect a security breach, I must immediately notify my Site Contact or BAS-Net Administrator.

USER CODE OF ETHICS

- A. BAS-Net Users must treat Partner Agencies with respect, fairness and good faith.
- B. Each BAS-Net User should maintain high standards of professional conduct in the capacity as a BAS-Net User.
- C. The BAS-Net User has primary responsibility for his/her Client(s).
- D. BAS-Net Users have the responsibility to relate to the Clients of other Partner Agencies with full professional consideration.

I understand and agree to comply with all the statements listed above.

BAS-Net User Signature Date

BAS-Net Site Contact Date

NOTE: *The BAS-Net Site Contact must sign all User Policy forms for the agency’s BAS-Net Users. Homeless Alliance of Western New York staff will sign the User Policy forms for Site Contacts*

**CLIENT CONSENT and
RELEASE OF INFORMATION AUTHORIZATION**
For Buffalo Area Service Network (BAS-Net)

This agency is asking your permission to share information about you with other agencies through the BAS-Net Community Database.

You may choose to share any or all of the following information by placing your initials next to the appropriate item.

- _____ General Information (including name, social security number, date of birth, citizenship, emergency contacts, gender, race, marital status, household composition)

- _____ Medical information (including mental health and alcohol/drug use but NOT HIV/AIDS status)

- _____ Service history

- _____ Military information

- _____ Legal history

- _____ Employment, skills, and income information

- _____ Residential/housing information

- _____ Other: _____

You may also specify which agencies you will allow access to your information.

My information may be shared with the following agencies:

I understand that I **may cancel this authorization at any time by written request**, but the cancellation will be active as of that date and not before it. I understand that this release is valid for one (1) year from the date of this document unless otherwise specified.

SIGNATURE OF CLIENT OR GUARDIAN

SIGNATURE OF WITNESS

DATE

DATE

Client Consent and Release of Information Authorization
Homeless Alliance of Western New York - Buffalo Area Service Network (BAS-Net)

_____ is a Partner Agency in the Buffalo Area Service Network (BAS-Net). BAS-Net is a management information system administered by the Homeless Alliance of Western New York (HAWNY). Authorized personnel at partner agencies will enter relevant client information into BAS-Net for use in improving service delivery as well as community research and planning efforts.

This form fully protects your rights to privacy. Before signing this form, you should:

1. Make sure the release is in your best interest. You have a right to inspect or copy the information to be disclosed.
2. Not sign the authorization as a requirement to receive services
3. Understand the information is limited to the items that you initial.
4. Please be aware that the above-named organization can not assure information will not be redisclosed by HAWNY. However, the Homeless Alliance of Western New York **will not disclose** your name and other identifying information (including SSN, citizen or immigration status, address, phone numbers, emergency contact, DOB, gender, race, marital status, household relationships) without a separate authorization from you.
5. Be aware that this authorization does not allow for the disclosure of information about the diagnosis or treatment of HIV/AIDS. A separate authorization form is required for such disclosures.
6. Know you may restrict the disclosure of specific information including by not limited to: your physical and mental health history, legal, military, employment and residential history, income, skills, and service plans/notes.
7. Know information about the services provided to you and the outcomes of these services may be collected for the purpose of improving the quality of care and services to you and other homeless individuals and their families.
8. Know that this authorization will be valid for one (1) year from the date of signing, unless revoked in writing before it expires. You can specify a shorter period of time.
9. Know you have a right to a copy of this authorization.

Please initial on the line next to each area that may be disclosed to HAWNY

- | | |
|-------|---|
| _____ | General Information (including name, social security number, date of birth, citizenship, emergency contacts, gender, race, marital status, household composition) |
| _____ | Medical information (including mental health/alcohol/drug use) |
| _____ | Military information |
| _____ | Legal history |
| _____ | Employment, skills, and income information |
| _____ | Residential/housing information |
| _____ | Service history, plans, and notes |

I authorize _____ to disclose the information as initialed above to the Homeless Alliance of Western New York (HAWNY) for the **limited purpose of identifying resource needs and improving services to homeless populations in Western New York.**

SIGNATURE OF CLIENT
(PARENT OR GUARDIAN if under 18 years of age.)

SIGNATURE OF WITNESS

DATE

DATE

CANCELLATION

I hereby cancel my permission for _____ to release information to the Homeless Alliance of Western New York. The cancellation becomes effective on the date signed. _____ is not required to retrieve information disclosed prior to the cancellation.

SIGNATURE OF CLIENT

(PARENT OR GUARDIAN if under 18 years of age.)

SIGNATURE OF WITNESS

DATE

DATE

REFUSAL

I hereby refuse to authorize _____ to release information to the Homeless Alliance of Western New York.

SIGNATURE OF CLIENT

(PARENT OR GUARDIAN if under 18 years of age.)

SIGNATURE OF WITNESS

DATE

DATE

CONSUMER NOTICE
For Buffalo Area Services Network (BAS-Net)

This Agency receives funding from the U.S. Department of Housing and Urban Development to provide services for homeless and near-homeless individuals and their families. A requirement of this funding is that the Agency participates in the Buffalo Area Services Network (BAS-Net), a system which collects basic information about clients receiving services in our community.

We collect personal information directly from you for reasons that are discussed in our privacy statement. We may be required to collect some personal information by law or by organizations that operate this program. Other personal information that we collect is important to run our programs, to improve services for homeless persons, and to better understand the needs of homeless persons. We only collect information that we consider to be appropriate. A copy of the BAS-Net Privacy Notice is available to any Client upon request.

As part of this system, you will have the ability to share your personal information with other area agencies that participate in the network by completing a "Client Consent and Release of Information" form. This will allow agencies to work in a cooperative manner to provide you with efficient and effective services.

Public Notice (Federal Register / Vol. 69, No. 146) / Effective August 30, 2004

(Also Available in Spanish)

PRIVACY PROTECTION NOTICE
For Buffalo Area Services Network (BAS-Net)

THIS NOTICE DESCRIBES HOW INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION.

Effective Date: _____

OUR DUTY TO SAFEGUARD YOUR PROTECTED INFORMATION

_____ collects information about the people who access services. When we meet with you, we will ask you for information about you and your family and enter it into a computer program called the Buffalo Area Services Network or BAS-Net. Although BAS-NET helps us to keep track of your information, personal information about you is considered “protected information.” We are required to protect the privacy of your identifying information and to give you notice about how, when, and why we may use it.

We are also required to follow the privacy practices described in this notice, although _____ reserves the right to change our privacy practices and the terms of this notice at any time.

HOW WE MAY USE AND DISCLOSE YOUR INFORMATION

We use and disclose collective information for a variety of community reports. We have a limited right to include some of your information for reports on homelessness and services needed by those who are homeless. Information that could be used to identify who you are will never be used for these reports. We will not turn your information over to a national database. For uses beyond reports, we must your written consent.

Please review the Client Consent and Release of Information Authorization form for details. You must sign the Client Consent and Release of Information Authorization form before we can share your information but you do not have to sign the form in order to receive services.

YOUR RIGHTS REGARDING YOUR INFORMATION

- You have the right to get services even if you choose not to participate in data sharing
- You have the right to know who has seen your information
- You have the right to see your information and to request changes to it.

Information about filing a BAS-Net-related concern is available at your location. If you would like to file a concern, please advise a staff member to receive information about the necessary steps.

(Also Available in Spanish)

USER LICENSE REQUEST
For Buffalo Area Services Network (BAS-Net)

Name of Requestor: _____
Name of Participating Agency: _____
Name of New User: _____
Job Title of New User: _____
Job Description of New User: _____

FOR HAWNY USE ONLY

Authorized By: _____
License Number: _____
Initial Login: _____
Initial Password: _____

Data Entry Training: _____
BAS-Net Level: _____
Security Question: _____
Security Answer: _____

REVOCACTION OF CONSENT
For Buffalo Area Services Network (BAS-Net)

I hereby revoke my consent to share personal information in the Buffalo Area Services Network (BAS-Net). The cancellation becomes effective on the date signed.

NAME OF CLIENT (PRINT)

SIGNATURE OF CLIENT (or PARENT OR GUARDIAN if under 18 years of age.)

SIGNATURE OF STAFF MEMBER CLOSING RECORD

DATE

My client has made an oral request to revoke his/her consent to share personal information in the Buffalo Area Services Network (BAS-Net). The cancellation becomes effective on the date signed.

NAME OF CLIENT (PRINT)

SIGNATURE OF STAFF MEMBER CLOSING RECORD

DATE

V. Glossary of Terms

Aggregated Data: Summary data from all, or a subset of community providers, on variable(s) of interest.

Audit Trail: An extensive auditing system that monitors, records and reports on what valid users of BAS-Net are doing.

Authentication: The process by which users validate their identity.

Confidentiality: 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 of confidential data include: social security number, name, address, or any other information that can be used to identify a client.

Emergency Shelter: Facility-based or scattered-site units that provide temporary shelter for homeless persons. clients may receive services to support their movement into transitional or permanent housing. They may have separate living quarters (room or apartment) or may have a congregate living situation such as dormitory-style.

Encryption: Conversion of plain text into encrypted data by scrambling it using a secret code that masks the meaning of the data to any unauthorized viewer. Computers encrypt data by using algorithms or formulas. Encrypted data are not readable unless they are converted back into plain text via decryption.

Encryption Solutions:

a.) **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.

b.) **Database:** Encryption that occurs at the field (data element) level within a record of information.

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

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

Penetration Testing: Process used to validate the security architecture used to protect a system.

Privacy: 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: Information that has been approved for public release by the BAS-Net Advisory Committee.

Restricted Data: Information not ever scheduled for publication.

Security: Protection of the client and program information stored in the HMIS from unauthorized access, use, or modification.