HOMELESS ADVOCACY FOR RURAL TENNESSEE

Homeless Management Information System (HMIS) Policies and Procedures 17-3

September 14, 2017

Replaces October 3, 2014 Edition

Table of Contents

HMIS Policies and Procedures Introduction

HMIS Lead Roles and Responsibilities

HMIS lead roles and responsibilities are found in the HART HMIS Charter.

Partner Agency Responsibilities

Partner agencies are expected to understand and comply with this Policy and Procedures.

ServicePoint Orientation

Some of the following procedures are worded based on using ServicePoint. If a new HMIS software is used, wording may need to be modified.

Source Documents

Homeless Management Information Systems (HMIS); Data and Technical Standards Final Notice, 2004

Homeless Management Information Systems Requirements, Proposed Rule 24 CFR Part 580, 2011

24 CFR Part 578, Continuum of Care Program Interim Rule, 2013

2014 Homeless Management Information Systems (HMIS); Data Standards 5.1, 2016

Network Data Sharing

The HART HMIS is considered an "open" network. Most agencies with direct services to the homeless have visibility to client demographics, entry (start)/exit information, and services. However, other information such as case management notes are not shared. This allows for avoidance of duplicate services, but still allows for some privacy in case management. There are projects that participation cannot be known do to federal rules such as HHS PATH projects. These projects cannot share entry (start)/exit or service information. Also, domestic violence service providers are forbidden to be on HMIS. There are other agencies that may request to be on HMIS that are not dedicated only to homeless persons such as organizations with a food pantry or provide utility or rent assistance. Their visibility settings will be not be set as freely as the direct homeless providers.

HMIS Implementation

HMIS Participation Policy

Mandatory Participation

All projects that are authorized under HUD's McKinney-Vento Act as amended by the HEARTH Act to provide homeless services must meet the minimum HMIS participation standards as defined by this policies and procedures manual. These participating agencies will be required to comply with all applicable operating procedures and must agree to execute and comply with an HMIS agency partner agreement.

Voluntary Participation

While Homeless Advocacy for Rural Tennessee (HART) cannot require non-funded providers to participate in the HMIS, it works closely with non-funded agencies to articulate the benefits of the HMIS and to strongly encourage their participation in order to achieve a comprehensive and accurate understanding of homelessness in the CoC.

Minimum Participation Standards

- ⇨ Each participating agency will execute an HMIS agency partner agreement (Annex E).
- ⇨ Agency staff will collect the universal and program-specific data elements as defined by HUD and other data elements as determined by the HMIS committee for all clients served by projects participating in HMIS; data may be shared with other agencies subject to appropriate client consent and network data sharing agreements.
- ⇨ Agency staff will enter client-level data into the HMIS in accordance to the data quality plan.
- ⇨ Participating agencies will comply with all HUD regulations for HMIS participation.
- ⇨ Each agency will designate at least one HMIS agency administrator. This person functions as the main liaison with the HMIS management team and is responsible for organizing his/her agency's end users, making sure proper training has taken place for the end users and that all paperwork and confidentiality requirements are being followed by all end users from that agency.

HMIS Partnership Termination-Data Transfer Policies

In the event that the relationship between HART HMIS and a partner agency is terminated, the partner agency will no longer have access to the HMIS. The HMIS management team will make reasonable accommodations to assist the partner agency to export its data in a format that is usable in its alternative database. Any costs associated with exporting the data will be the sole responsibility of the partner agency.

HMIS Agency Implementation

Adding Partner Agencies

Prior to setting up a new partner agency within the HMIS database, the HMIS management team will:

- ⇨ Review HMIS records to ensure that the agency does not have previous violations
- ⇨ Verify that the required documentation has been correctly executed and submitted or viewed on site, including:
  - Partner agreement
  - Additional documentation on agency and project(s)
  - Designation of HMIS agency administrator
  - Fee payment, if applicable
- ⇨ Work with the partner agency to input applicable agency and project information
- ⇨ Work with the partner agency to migrate legacy data, if applicable

Agency Information Security Protocol Requirements

At a minimum, partner agencies must develop security rules, protocols, or procedures based on the *HUD Data and Technical Standards, Final Notice,* including but not limited to the following:

- ⇨ Internal agency procedures for complying with the HMIS privacy notice and provisions of other HMIS client and agency agreements
- ⇨ Maintaining and posting an updated copy of the agency's privacy notice on the agency's website
- ⇨ Posting a sign in the areas of client intake that explains generally the reasons for collecting personal information
- ⇨ Preventing user account sharing
- ⇨ Protection of unattended workstations
- ⇨ Protection of physical access to workstations where employees are accessing HMIS
- ⇨ Safe storage and protected access to hardcopy and digitally generated client records and reports with identifiable client information
- ⇨ Proper data cleansing of equipment prior to transfer or disposal
- ⇨ Procedures for regularly auditing compliance with the agency's information security protocol

The HMIS management team conducts semi-annual site visits to monitor compliance with HMIS policies, at which time agencies may need to demonstrate their procedures for securing client data.

HMIS User Implementation

Eligible Users

Partner agencies are expected to have conducted background checks on any end user that issued an HMIS license. And, it is expected that each partner agency will authorize use of the HMIS only to users who need access to the system for data entry, editing of client records, viewing of client records, report writing, administration, or other essential activity associated with carrying out participating agency responsibilities.

End User Requirements

Prior to being granted a username and password, end users must sign an HMIS confidentiality agreement (See Annex D).

End users must be aware of the sensitivity of client-level data and must take appropriate measures to prevent its unauthorized disclosure. End users are responsible for protecting institutional information to which they have access and for reporting security violations. End users must comply with all policies and standards described within this policies and procedures manual. They are accountable for their actions and for any actions undertaken with their username and password.

The HMIS management team must ensure that end users have received adequate training prior to being given access to the system.

Setting Up a New End User

If the partner agency wants to authorize system use for a new end user, the agency's executive director or authorized designee must coordinate with the HMIS management team to:

- ⇨ Determine the access level of the proposed HMIS user,
- ⇨ Execute an HMIS end user confidentiality agreement,
- ⇨ Review HMIS records about previous end users to ensure that the individual does not have previous violations with the HMIS policies and procedures that prohibit their access to the HMIS, and
- ⇨ Verify that appropriate and sufficient training has been successfully completed.

Volunteers have the same user requirements that paid staff have. They must have an individual license, go through the same training, and have the same confidentiality and privacy documents signed and on file with the HMIS office and/or the agency they are serving.

The executive director or authorized designee is responsible for ensuring that the user understands and complies with all applicable HMIS policies and procedures.

Removing an End User

If any end user leaves the agency or no longer needs access to the HMIS, the partner agency is responsible for notifying the HMIS management team to immediately terminate user access by deleting or inactivating the user account.

Enforcement Mechanisms

Partner agency or end user access may be suspended or revoked for suspected or actual violation of the security protocols.

The following steps will be taken as appropriate:

- ⇨ All suspected violations of any security protocols will be investigated by the agency and the HART HMIS management team.
- ⇨ Any user found to be in violation of security protocols will be sanctioned by his/her agency. 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/or criminal prosecution.
- ⇨ Access may be restricted prior to completion of formal investigation if deemed necessary by the HMIS lead. If access is restricted, the HMIS lead will notify the HMIS committee chair of the restriction and will consult with him/her about next steps.
- ⇨ Any agency that is found to have consistently and/or flagrantly violated security protocols may have their access privileges suspended or revoked.
- ⇨ All sanctions can be appealed to the HART HMIS Committee.

HMIS License Management

The HMIS lead will manage all the licenses within the HART HMIS. If the HMIS implementation changes to a structure in which all agencies pay for all their licenses, then the individual agency administrators will control the licenses that they have purchased.

Under the current HMIS grant structure, the HMIS grant has enough funding to pay for the HMIS licenses necessary to administer the system in the CoC. The HMIS lead will work with partner agencies to determine how many free licenses will be available to the partner agency. The general rule is that a free license will be offered for each CoC, ESG, SSVF, and PATH project. Additional licenses may be offered based on size and structure of the projects within the agencies. Other licenses will be freely offered to other agencies that are not federally funded but are a significant part of the CoC system such as homeless shelters, homeless transitional housing, and other projects with direct services to homeless populations. Additional licenses that are not currently assigned may also be used for agencies that may serve homeless persons but that is not the primary aim of the project such as food pantries.

If a partner agency desires more licenses than the HMIS lead will provide freely, it will be required to purchase them. Any licenses purchased will be on an annual basis without refund.

A partner agency may lose its access to HMIS due to inactivity. The following steps will be taken as appropriate:

1. HMIS office will monitor logons and data input into the HMIS.
2. If a user has not logged in and contributed data into HMIS in over 90 days, the HMIS Lead will send a letter to the partner agency's HMIS administrator that the license is at risk of being removed. If the administrator provides adequate explanation or the user begins activity within 30 days, the case is closed.
3. If a user has not contributed data into HMIS in over 120 days or the partner agency HMIS administrator does not provide adequate explanation for the inactivity, then a second letter will be sent to the partner agency executive director (or equivalent) and will be copy furnished to the HMIS committee chair. This letter will inform the executive director the concern and request if the partner agency or the licensed user is no longer required or desires to be on HMIS.
4. If a user has not contributed data into HMIS in over 150 days or the partner agency executive director does not provide adequate explanation for the inactivity, another letter will be sent to the partner agency executive director and copy furnished to the HART board of director's chair. This letter will state that the license is suspended and will be removed in 30 days.

DATA ACCESS CONTROL POLICIES

User Passwords

Each user will be assigned a user name, preferably the first initial and last name of the user.

A temporary password will be assigned when a new user account is created. The user will be required to establish a new password upon initial log-in. This password automatically expires every 45 days. Passwords must be between 8 and 16 characters long, contain at least two numbers, and should not be easily guessed or found in a dictionary. The password format is alphanumeric and is case-sensitive.

Users are prohibited from sharing passwords—even with supervisors. Sanctions will be imposed on the user and/or agency if user account sharing occurs. Any passwords written down should be securely stored and inaccessible to others. They should not be saved on a personal computer.

Password Reset

End users can reset their own password once logged on by editing their profile (gear symbol). The HMIS management team and the agency administrator have the ability to reset passwords.

Temporary Suspension of User Access to HMIS

System Inactivity

Users must log off from the HMIS application and either lock or log off their respective workstation if they leave the workstation. Also, password protected screen-savers or automatic network log-off should be implemented on each workstation. If the user is logged into HMIS and the period of inactivity in HMIS exceeds 30 minutes, the user will be logged off the HMIS automatically.

Unsuccessful Log-in

If a user attempts to log in 3 times unsuccessfully, the account will be "locked out." The user will be unable to regain access until the password is reset by the agency administrator or a member of the HMIS management team.

Electronic Data Control

Agency Policies Restricting Access to Data

Partner agencies must establish protocols limiting internal access to data based on the final *HUD Data and Technical Standards* (See HMIS Security Plan in this Policy and Procedures).

Downloaded Data

Users have the ability to download and save client-level data. Once this information has been downloaded from the HMIS server, the security of this data then becomes the responsibility of the user and the agency.

Hardcopy Data Control

Printed versions (hardcopy) of confidential data should not be copied or left unattended and open to compromise. Media containing HMIS client-identified data will not be shared with any agency, other than the owner of the data, for any reason. Authorized employees using methods deemed appropriate may transport HMIS data between the participating agencies that meet the above standard. Reasonable care should be taken, and media should be secured when left unattended. Magnetic media containing HMIS data which is released and/or disposed of by the participating agency and the central server should first be processed to destroy any data residing on that media. Degaussing and overwriting are acceptable methods of destroying data. HMIS information in hardcopy format should be disposed of properly. This could include shredding finely enough to ensure that the information is unrecoverable.

HMIS Privacy Policy

ALLOWABLE HMIS USES AND DISCLOSURES

Each of the HMIS partner agencies must comply with the following uses and disclosures, as outlined in the *HUD Data and Technical Standards: Final Notice.* A partner agency has the right to establish additional uses and disclosures as long as they do not conflict with these uses and disclosures.

Identifiable HMIS client data may be used or disclosed for case management, billing, administrative and analytical purposes.

- ⇨ To provide or coordinate services to a client
- ⇨ For functions related to payment or reimbursement for services
- ⇨ To carry out administrative functions, including but not limited to legal, audit, personnel, oversight and management functions
- ⇨ For functions that are related to analyzing client data to understand homelessness, including but not limited to creating de-identified protected personal information, understanding trends in homelessness and the needs of persons who are homeless, and assessing the implementation of the Continuum's Strategic Plan to End Homelessness
- ⇨ Where the disclosure is required by law and the disclosure complies with and is limited to the requirements of the law
- ⇨ If the individual agrees to the disclosure
- ⇨ To the extent that the disclosure is expressly authorized by statute or regulation; and the partner agency believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or if the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the protected personal information (PPI) for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure
- ⇨ The partner agency, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm
- ⇨ The partner agency would be informing a personal representative (such as a family member or friend), and the partner agency reasonably believes the personal representative is responsible for the abuse, neglect or other injury, and that informing the personal representative would not be in the best interests of the individual as determined by the partner agency, in the exercise of professional judgment
- ⇨ A partner agency may use or disclose PPI for academic research conducted by an individual or institution that has a formal relationship with the partner agency if the research is conducted either:

- By an individual employed by or affiliated with the organization for use in a research project conducted under a written research agreement approved in writing by a program administrator (other than the individual conducting the research) designated by the partner agency; or
- By an institution for use in a research project conducted under a written research agreement approved in writing by a program administrator designated by the partner agency.

  A written research agreement must: (1) Establish rules and limitations for the processing and security of PPI in the course of the research; (2) provide for the return or proper disposal of all PPI at the conclusion of the research; (3) restrict additional use or disclosure of PPI, except where required by law; and (4) require that the recipient of data formally agree to comply with all terms and conditions of the agreement. A written research agreement is not a substitute for approval of a research project by an Institutional Review Board, Privacy Board or other applicable human subjects protection institution.

⇨ Disclosures for law enforcement purposes in response to a lawful court order, court-ordered warrant, subpoena or summons issued by a judicial office or a grand jury subpoena

COLLECTION LIMITATION

Partner agencies may collect protected personal information only when appropriate to the purposes for which the information is obtained or when required by law.

A partner agency must collect PPI by lawful and fair means and, where appropriate, with the knowledge or consent of the individual. The participating agency must post a sign at each intake desk (or comparable location) that explains generally the reasons for collecting this information (Annex A). Consent of the individual for data collection may be inferred from the circumstances of the collection.

DATA QUALITY

PPI collected by a partner agency must be relevant to the purpose for which it is to be used. To the extent necessary for those purposes, PPI should be accurate, complete and timely.

A partner agency must develop and implement a plan to dispose of or, in the alternative, to remove identifiers from, PPI that is not in current use seven years after the PPI was created or last changed (unless a statutory, regulatory, contractual, or other requirement mandates longer retention).

PURPOSE SPECIFICATION AND USE LIMITATION

HART has prepared standard documents for HMIS Notice of Privacy Practices and Client Consent to Release Information which are available in Annexes B and C. Partner agencies may either use these forms or incorporate the content of the HMIS documents into the agency's own documentation. All written consent forms must be stored in each client's case management file for record keeping and auditing purposes.

OPENNESS

Each partner agency must publish a privacy notice that incorporates the content of the *HUD Data and Technical Standards: Final Notice* as described below. Sample may be found in Annex B.

Each agency must post a sign stating the availability of the privacy notice and provide a copy of it to any client upon request. If an agency maintains a public web page, the agency must post the current version of its privacy notice on its web page.

An agency's privacy notice must:

- ⇨ Specify all potential uses and disclosures of a client's personal information
- ⇨ Specify the purpose for collecting the information
- ⇨ Specify the time period for which a client's personal information will be retained at the agency
- ⇨ Specify the method for disposing of a client's personal information or removing identifiers from personal information that is not in current use seven years after it was created or last changed
- ⇨ State the process and applicability of amendments and commit to documenting all privacy notice amendments
- ⇨ Offer reasonable accommodations for persons with disabilities and/or language barriers throughout the data collection process
- ⇨ Allow the individual the right to inspect and to have a copy of his/her client record and offer to explain any information that the individual may not understand
- ⇨ Specify a procedure for accepting and considering questions or complaints about the privacy and security policies and practices

Agencies must make reasonable accommodations for persons with disabilities throughout the data collection process. This may include, but is not limited to, providing qualified sign language interpreters, readers or materials in accessible formats such as Braille, audio or large type, as needed by the individual with a disability.

Agencies that are recipients of federal assistance will provide required information in languages other than English that are common in the community if speakers of these

languages are found in significant numbers and come into frequent contact with the project.

Access and Correction Standards

In general, a partner agency must allow an individual to inspect and to have a copy of any PPI about the individual. A partner agency must offer to explain any information that the individual may not understand. A partner agency must consider any request by an individual for correction of inaccurate or incomplete PPI pertaining to the individual. A partner agency is not required to remove any information but may, in the alternative, mark information as inaccurate or incomplete and may supplement it with additional information.

In its privacy notice, a partner agency may reserve the ability to rely on the following reasons for denying an individual inspection or copying of the individual's PPI: (1) Information compiled in reasonable anticipation of litigation or comparable proceedings; (2) information about another individual (other than a health care or homeless provider); (3) information obtained under a promise of confidentiality (other than a promise from a health care or homeless provider) if disclosure would reveal the source of the information; or (4) information, the disclosure of which would be reasonably likely to endanger the life or physical safety of any individual.

A partner agency can reject repeated or harassing requests for access or correction. A partner agency that denies an individual's request for access or correction must explain the reason for the denial to the individual and must include documentation of the request and the reason for the denial as part of the protected personal information about the individual.

Accountability

A partner agency must establish a procedure for accepting and considering questions or complaints about its privacy and security policies and practices. A partner agency must require each member of its staff (including employees, volunteers, affiliates, contractors and associates) to sign (annually or otherwise) a confidentiality agreement that acknowledges receipt of a copy of the privacy notice and that pledges to comply with the privacy notice.

Protection for Victims of Domestic Violence, Dating Violence, Sexual Assault and Stalking

An agency that is serving a victim of domestic violence, dating violence, sexual assault or stalking are not allowed to participate in HMIS; however, may be required by their funding agency to maintain the same universal data elements on an alternative database system. The guidelines established by this manual should be considered minimal requirements. Because of the nature of domestic violence, it is expected that these support programs will maintain additional safeguards.

UNACCOMPANIED MINOR YOUTH

Based on their age and potential inability to understand the implications of sharing information, the HMIS cannot be used to share information about unaccompanied minor youth outside of the originating agency. Thus, even with written client authorization, users cannot share any client information of unaccompanied minor youth. For the purposes of this policy, minor youth are defined as youth under 18 years of age unless legally emancipated.

PRIVACY COMPLIANCE AND GRIEVANCE POLICY

Clients of partner agencies will use its existing grievance procedures regarding unsatisfactory services or use and disclosure of personal protected information (PPI) in the HART HMIS as these issues are most likely within a partner agency. It is only when the issue involves the actions of the HART HMIS CoC operation that the HART HMIS grievance procedure is to be used. Additionally, the HART HMIS grievance procedure is not intended for use as an "appeal" for a local decision.

If a client wants to file a complaint, s/he needs to follow these steps:

1. The client complaint is to be brought to the attention of the partner agency's Executive Director or designee who will assist the client in the grievance procedure.
2. The complaint is to be stated in writing.
3. The complaint will be passed to the HART HMIS chief administrator.
4. The client and the partner agency's representative meet together with the HART HMIS chief administrator to resolve the complaint.
5. The actions and resolutions will be in writing.
6. Should the client want to appeal the HMIS lead agency's decision, the HART chair will form an ad hoc grievance committee to address the complaint. The committee must have at least one person from the HMIS committee and one person who is not on the HMIS committee. The chair will convene the committee by person, teleconference, or by email to review the complaint. The committee will contemplate the validity of the complaint and determine if established policies and procedures have been violated or if they should be amended to comply with regulatory requirements or good business practices.
7. All decisions of HART's adhoc grievance committee are final.

HMIS Data Quality Plan

DATA TIMELINESS

All data will be entered into the HMIS in a timely manner. HUD is now monitoring CoC-funded projects on the timeliness of HMIS data input, but has not set any specific standards. Because of the distance between projects on this HMIS, there is very little overlap in clients and very low risk of an attempt at duplication of services so the CoC is adopting a lenient policy on when data must be entered into HMIS. The CoC-funded housing projects require an APR after completing a renewable grant, and there is a report on timeliness in this APR. It is in the best interest of the agency to enter data into HMIS as soon as possible; however, the CoC standard is to enter the data is within 14 days of entry/start of a project.

DATA COMPLETENESS

All data entered into the HMIS will be complete. The continuum's goal is to collect 100% of all required data elements. However, the continuum recognizes that this may not be possible in all cases. Therefore, it has established an acceptable range of null/missing and unknown/don't know/refused responses of between 0 and 5 percent, depending on the data element and the type of program entering data. Complete HMIS data is necessary to fully understand the demographic characteristics and service use of persons in the system. Complete data facilitates confident reporting and analysis on the nature and extent of homelessness, such as:

- ⇨ Unduplicated counts of clients served at the local level,
- ⇨ Patterns of use of people entering and exiting the homeless assistance system, and
- ⇨ Evaluation of the effectiveness of homeless systems.

In effect, complete data tells the full "story" of homelessness to the agencies, the continuum, and the general public. Complete data also helps the continuum meet funded compliance requirements.

DATA ACCURACY

The purpose of accuracy is to ensure that the data in the CoC's HMIS is the best possible representation of reality as it relates to homeless people and the programs that serve them. To that end, all data entered into HART's HMIS will be a reflection of information provided by the client, as documented by the intake worker or otherwise updated by the client and documented for reference. Recording inaccurate information is strictly prohibited. All data in HMIS will be collected and entered in a common and consistent manner across all programs. To that end, all intake and data entry workers will complete an initial training before accessing the live HMIS system. All HMIS users must recertify their knowledge of consistency practices on an annual basis. A basic intake form that collects data in a consistent manner will be available to all programs, which they can alter to meet their additional needs, provided the base document does not change.

Data Monitoring

HART recognizes that the data produced from the HMIS is critical to meet the reporting and compliance requirements of individual agencies and the CoC as a whole. As such, all HMIS agencies are expected to meet the data quality benchmarks described in this document. To achieve this, the HMIS data will be monitored on a monthly basis to quickly identify and resolve issues that affect the timeliness, completeness, and accuracy of the data.

Data Quality Training

End User Training

Each end user of the HMIS must complete HMIS training before being given HMIS log-in credentials. HART HMIS management team will train all end users to ensure consistency across the continuum.

Reports Training

Reports training for agency administrators and other interested users will be made available as needed. These will include training on how to use reporting tools in ServicePoint.

Agencies are expected to run their own data quality reports so that they can monitor their own data quality and become more effective in serving our clients across the continuum.

System Performance Measures (Data Metrics)

HUD is requiring the following metrics to be reported.

- ⇨ Length of Time Persons Remain Homeless
- ⇨ Exits to Permanent Housing with Return to Homelessness
- ⇨ Number of Homeless Persons
- ⇨ Employment and Income Growth for CoC Program-funded Projects
- ⇨ Number of Persons Who Become Homeless for the First Time
- ⇨ Permanent Housing Placement-Retention

HMIS Technical Support

HMIS Technical Support Policies and Procedures

HMIS Application Support

As unanticipated technical support questions on the use of the HMIS application arise, users will follow this procedure to resolve those questions:

- ⇨ Begin with utilization of the on-line help and/or training materials
- ⇨ If the question is still unresolved, direct the technical support question to the agency administrator
- ⇨ If the question is still unresolved, the Agency Administrator or end user can direct the question to the HMIS management team
- ⇨ If the question is still unresolved, the HMIS management team will direct the question to Bowman Systems technical support staff

User Training

The HMIS management team will provide HMIS application training periodically throughout the year. If additional, or specific, training needs arise, the HMIS management team may arrange for special training sessions.

Agency/User Forms

All Agency Administrators will be trained in the appropriate on-line and hardcopy forms. If the agency administrator has questions on how to complete HMIS forms, s/he will contact the HMIS management team.

Report Generation

Each agency may send its agency administrator to receive training on how to develop agency-specific reports using the HMIS application. The HMIS management team will be a resource to agency users as they develop reports.

HMIS Availability Policies

There are times that ServicePoint is unavailable because Bowman Systems is performing necessary backup and maintenance of the HMIS database. These are usually in the late evenings when as few people as possible need access to the system.

However, when HART receives notice of a planned interruption of service for other reasons or for an abnormal amount of time, the HMIS management team will notify agency administrators via email. If there is an unplanned interruption to service, the HMIS management team will communicate with Bowman Systems, and agency administrators will be notified of any information regarding the interruption as it is made available.

HMIS Security Plan

HARDWARE, CONNECTIVITY AND COMPUTER SECURITY REQUIREMENTS

Workstation Specification

Computers should meet the **minimum** desktop specification:

- ⇨ Operating System: Any system capable of running a current Internet browser as specified below except MS Windows prior to Windows 7.
- ⇨ Processor: 2 GHz Pentium processor or higher; dual core recommended.
- ⇨ Memory: 4 GB recommended (2 GB minimum).
- ⇨ Web Browsers: MS Internet Explorer, Chrome, Mozilla Firefox, or Apple Safari. When these browsers have significant updates or replacements, there will be a period of time before Bowman Systems can certify their use with ServicePoint.

Internet Connectivity

Partner agencies must have Internet connectivity for each workstation accessing the HMIS. To optimize performance, all agencies are encouraged to secure a high-speed Internet connection with a cable modem, DSL or T1 line. Agencies expecting a very low volume of data may be able to connect using a dial-up connection; however, HMIS management cannot guarantee satisfactory performance with this option.

Security Hardware/Software

All workstations accessing the HMIS need to be protected by a securely configured firewall. If the workstations are part of an agency computer network, the firewall may be installed at a point between the network and the Internet or other systems rather than at each workstation. Each workstation also needs to have anti-virus and anti-spyware programs in use and properly maintained with automatic installation of all critical software updates.

Agency Workstation Access Control

Each partner agency will determine the physical access controls appropriate for their organizational setting based on HMIS security policies, standards and guidelines. Each workstation, including laptops and other mobile devices used off site, should have appropriate and current firewall and virus protection as specified above under *Security Hardware/Software.*

ANNEX A - Sample Sign at Protected Personal Information Intake Location

A partner agency must post a sign at each intake desk (or comparable location) that explains generally the reasons for collecting protected personal information (PPI). Below are two samples. Sample 1 contains the required information for the sign. This can be modified, but each principle must remain.

SAMPLE TEXT FOR POSTING AT ENTRY (SAMPLE 1)

Providers may wish to use the following language to assure that they meet this HUD's baseline standard:

''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 give us money to 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."

CONSUMER NOTICE (SAMPLE 2)

Homeless Advocacy for Rural Tennessee (HART) Homeless Information Management System (HMIS)

This Agency receives funding from U.S. Department of Housing and Urban Development to provide services for homeless and at risk of becoming homeless individuals and their families. A requirement of this funding is that the Agency participates in the HART HMIS which collects basic information about clients receiving services from this Agency. This requirement was enacted in order to get a more accurate count of individuals and families who are homeless and to identify the need for different services.

We only collect information that we consider to be appropriate. The collection and use of all personal information is guided by strict standards of confidentiality. A copy of our Privacy Notice describing our privacy practice is available to all consumers upon request.

You do have the ability to share your personal information with other area agencies that participate in the system by completing a "Release of Information" form. This will allow those agencies to work in a cooperative manner to provide you with efficient and effective services.

ANNEX B - Sample Partner Agency Privacy Notice

{Partner Agency}'s Homeless Management Information System (HMIS):

When you request services from this agency, we will enter information about you and your family into the Homeless Management Information System (HMIS), a computer database commonly referred to as HMIS. This HMIS is administered by Homeless Advocacy for Rural Tennessee (HART). The HMIS is used by many agencies throughout the Upper Cumberland that provide services to persons and families in need. The information collected in the HMIS will help us reduce duplicate intakes, document the need for services, and generate reports such as the number of persons who are homeless in the region.

How your information in the HMIS may be used or disclosed:

Unless restricted by other laws, your information will be used: (1) to provide individual case management, services, and/or treatment to you at this agency and other agencies that use the HMIS; (2) for statistical purposes, such as determining the number of persons that are homeless; (3) to track individual program-level outcomes; (4) to identify unfilled service needs and plan for the provision of new services; (5) to obtain payment for services provided to you; (6) for quality assessment, training, evaluation, legal and business planning, and other health-care operations; (7) to allocate resources among agencies engaged in the provision of services; and (8) other uses allowed by law.

The information about you can also be used by or disclosed to the following:

- To provide or coordinate services to a client
- For functions related to payment or reimbursement for services
- To carry out administrative functions, including but not limited to legal, audit, personnel, oversight and management functions
- For functions that are related to analyzing client data to understand homelessness, including but not limited to creating de-identified protected personal information, understanding trends in homelessness and the needs of persons who are homeless, and assessing the implementation of the Continuum's Strategic Plan to End Homelessness
- Where the disclosure is required by law and the disclosure complies with and is limited to the requirements of the law
- If the individual agrees to the disclosure
- To the extent that the disclosure is expressly authorized by statute or regulation; and the partner agency believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or if the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the PPI for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure
- The partner agency, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm
- The partner agency would be informing a personal representative (such as a family member or friend), and the partner agency reasonably believes the personal representative is responsible for the abuse, neglect or other injury, and that informing the personal representative would not be in the best interests of the individual as determined by the partner agency, in the exercise of professional judgment
- A partner agency may use or disclose PPI for academic research conducted by an individual or institution that has a formal relationship with the partner agency if the research is conducted either:
    - By an individual employed by or affiliated with the organization for use in a research project conducted under a written research agreement approved in writing by a program administrator (other than the individual conducting the research) designated by the partner agency; or

- By an institution for use in a research project conducted under a written research agreement approved in writing by a program administrator designated by the partner agency.

Other uses and disclosures of your information will be made only with your written consent. You may revoke your consent at any time in writing, except if the agency has already released information as a result of your consent.

Your rights regarding your information in the HMIS:

- You have the right to inspect and obtain a copy of your own protected personal information for as long as it is kept in the HMIS, except for: (1) Information compiled in reasonable anticipation of litigation or comparable proceedings; (2) information about another individual (other than a health care or homeless provider); (3) information obtained under a promise of confidentiality (other than a promise from a health care or homeless provider) if disclosure would reveal the source of the information; or (4) information, the disclosure of which would be reasonably likely to endanger the life or physical safety of any individual.
- You have the right to request that your protected personal information is corrected when the information in the record is inaccurate or incomplete.
- You have a right to request that your personal information be provided to you by alternative means (such as by mail or telephone) or at alternate locations (such as at your home or place of work). This agency will accommodate reasonable requests.
- You have the right to receive a list of disclosures of your protected personal information made by this agency during the six (6) years prior to the date you request this information, except for disclosures for national security or intelligence purposes or to correctional institutions or law enforcement officials. If a law enforcement official or health oversight agency requests that we temporarily suspend giving you an accounting of disclosures made to them, the request must be time-limited and given to us in writing.

Exercising your rights regarding your information in the HMIS:

You can exercise these rights by making a written request to this agency or by making a written request to HART. The addresses are listed at the end of this notice.

Enforcement of your privacy rights:

If you believe your privacy rights have been violated, you may send a written complaint to this agency. If your complaint is not resolved to your satisfaction, you may send your written complaint to HART. Addresses are listed at the end of this notice. You will not be retaliated against for filing a complaint.

This agency is required by law to maintain the privacy of your protected personal information and to display a copy of the most recent HMIS Notice of Privacy Practice ("Notice"). This Agency reserves the right to change this Notice from time to time, and if it does, the change will affect all of the information in the HMIS, not just the information entered after the change. The revised Notice will be posted by this Agency. You may request a copy of it from this Agency.

PPI destruction:

PPI that is not in current use will be destroyed or de-identified seven years after it was created or last changed.

ANNEX C - Sample Release of Information (ROI)

HMIS Information Management System
Client Release of Information Form

I/we, _____,
give permission to [agency] to share information collected to other agencies participating in Homeless Advocacy for Rural Tennessee Continuum of Care Homeless Management Information System for the purposes of improving services available to me and collecting non-personal data on homeless individuals and families. I also understand that this information is kept confidential and that this release is good for one year and one day from today. This agreement may be revoked at any time by submitting a written request to this agency. This authorization is not required to receive benefits from this agency.

_____ _____/_____/_____
(Signature) (Date)

_____ _____/_____/_____
(Signature) (Date)

Children covered by this release of information:

_____
_____
_____
_____
_____
_____
_____

ANNEX D - HMIS End User Confidentiality Agreement

Name _____AGENCY_____
Print

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 the HART HMIS.

_____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 the HART HMIS are authorized users and the clients to whom the information pertains.

_____I understand that written client authorization to share data is required before identifying client information is shared.

_____I understand that there is a grievance policy for clients who believe that their protected personal identification (PPI) isn't properly controlled.

_____I acknowledge that I have been informed that my agency must have a privacy notice and to pledge to comply with the privacy notice as issued.

_____I may only view, obtain, disclose, or use the database information that is necessary to perform my job. I may access client information only to retrieve data relevant to a client requesting services from my agency.

_____I understand that a computer that has the HART HMIS open and running will never be left unattended. Therefore if I am logged on and must leave the work area where the computer is located, I must log-off of the system before leaving the work area in order to protect client confidentiality and system security. Failure to log off HART HMIS appropriately may result in a breach in client confidentiality and system security.

_____Hard copies of HART HMIS information must be kept in a secure file. When hard copies of HART HMIS information are to be discarded, they must be properly destroyed according to my agency's policy in order to maintain confidentiality.

_____If I notice or suspect a security breach, I must immediately notify the HMIS management team.

_____I have read and will abide by my agency's Privacy Notice.

_____

HART HMIS User Signature Date

ANNEX E - HMIS Memorandum of Understanding

MEMORANDUM OF UNDERSTANDING
between
Homeless Advocacy for Rural Tennessee Homeless Management Information System Lead
and
{Partner Agency}

Homeless Advocacy for Rural Tennessee (HART) HMIS Lead will:

- Oversee and coordinate all aspects of the HART HMIS Project's implementation and development;
- Serve as the primary contact with the HMIS vendor;
- Monitor the vender's performance under their contract with HART;
- Provide ongoing training on the use of the HMIS software;
- Oversee system administration especially as it relates to external security protocols;
- Oversee and coordinate the activities of the agency administrator; and
- Provide support to and function as a resource to the end users and the agency administrator.

***{Partner Agency}* will appoint at least one person to serve as the HMIS Agency Administrator for the agency, and this person will:**

- Oversee all agency staff who have access to or generate client-level data;
- Permit only those staff who are certified by HART to use the HMIS software and authorize as users only those staff who need access to the system for data entry, editing of client records, viewing of client records, report writing, administration or other essential activities related to the use of it;
- Ensure that each end user has read the HART HMIS End User Section, signed the End-User Agreement, and is in compliance with the policies and procedures;
- Ensure that each end user has his/her own software license;
- Assume responsibility for the integrity and protection of client-level data entered at their site;
- Ensure to the extent possible that all data is entered accurately and timely;
- Maintain agency computer equipment and access to the internet;
- Edit and update agency information in HMIS;
- Notify all end users in their agency of interruptions in service;
- Serve as point-person in communicating with the HART HMIS Systems Administrator;
- Detect and respond to violations of the Policies and Procedures or agency procedures;
- Secure a release of information from clients to share personal information with other agencies within the CoC HMIS;
- Coordinate with HART HMIS on changes in license assignments and end-user level of access;
- Ensure that data is collected in a way that respects the dignity of the participants, and
- Inform all end users at their agency of the following:

"Users are any persons who use the HMIS software for data processing services. They must be aware of the data's sensitivity and take appropriate measures to prevent unauthorized disclosure. Users are responsible for protecting institutional information to which they have access and for reporting security violations. Users must comply with the policies and standards of the agency as they relate to security and confidentiality of the data. Users are legally accountable for their actions and for any actions undertaken with their usernames and passwords."

HART and the partner agency agree that their mutual participation in HART HMIS will cause each party to possess information that is confidential and which, in some cases, may be subject to special protections under state and federal law.

HART HMIS Initials_____ Participating Agency Initials_____

License Cost and Termination: The HMIS Lead with consultation with the HART HMIS Committee determines the cost of individual licenses. Since a license cannot be returned to the HMIS software vendor for a prorated refund, agencies that paid for their licenses will not get a refund if they return their license(s) prior to the new contract year between the vendor and the HMIS Lead.

Confidentiality Obligations: The partner agency agrees to hold all client information, which is disclosed or entered into the HART HMIS confidential. The partner agency agrees to take all reasonable steps to ensure that the confidential information is not disclosed or distributed by its Board members, employees, or volunteers to a third party, except as permitted by signed consent. The partner agency agrees, unless required by law, not to make such confidential information available in any form to any third party for any purpose other than for the implementation of and participation in the HART HMIS Project.

The partner agency will only have access to client-identifying data that has been expressly released by the client, as noted in the electronic case record. In addition to documentation in the client's electronic record, authorization to release information will be established through a written, signed Release of Information Form to be obtained by the partner agency from the client and retained in the partner agency's files.

HART will have access to all client information that has been entered into HART HMIS and agrees to maintain the security and confidentiality of such information as required by applicable laws and regulations, including the Health Insurance Portability and Accountability Act (HIPAA), the regulations promulgated thereunder, and applicable state law. HART will not use protected health information or any other confidential information for any other purpose except that of managing and administering the HART HMIS.

Indemnification: The partner agency agrees to indemnify, defend, and hold harmless HART against all losses, expenses, damages and costs arising out of the agency's participation in HART HMIS, excluding incidents of negligence and willful malfeasance.

HART agrees to indemnify, defend, and hold harmless the partner agency against all losses, expenses, damages and costs arising out of HART's participation in HART HMIS, excluding incidents of negligence and willful malfeasance.

No Warranty: HART's coordination of HART HMIS, including without limitation all services, functions, materials, content, and information, is provided "as is" without warranties of any kind, either express or implied.

Liability: In no event will HART Board members or employees be held liable for interruptions of services related to the use or inability to use the HMIS software or HART HMIS, or for the transmission of inaccurate information or a breach of security and/or confidentiality resulting from any malfunction of hardware or electronic communications system.

Neither will the partner agency or its Board members, staff, or volunteers be held liable for interruptions of services related to the use or inability to use the HMIS software or HART HMIS, or for the transmission of inaccurate information or a breach of security and/or confidentiality resulting from any malfunction of hardware or electronic communications system.

Release: The partner agency agrees to and does hereby release HART from any and all liability related to HART's performance under the MOU or the HART HMIS Project.

HART agrees to and does hereby release the partner agency from any and all liability related to the HART HMIS agency's performance under the MOU or the HART HMIS Project.

HART HMIS Memorandum of Understanding- Signature Page
HART and Covered Homeless Organization

By signing below I agree to the stipulations of this Memorandum of Understanding and agree that my agency will abide by the HART HMIS Policies and Procedures Manual.

HMIS Lead for Homeless Advocacy for Rural Tennessee

Signature: _____ Date: _____

Print Name: _____

Executive Director of {partner agency}

Executive Director's Signature: _____ Date: _____

Email of Executive Director: _____

Print Name: _____

Name of Agency: _____

Mailing Address: _____

Agency Programs Covered by MOU (Please write the names of the programs as they should appear in HART HMIS)
_____

_____

_____

Name of HMIS Administrator: _____

Title of HMIS Administrator: _____

Email of HMIS Administrator: _____