The Community Partnership For The Prevention of Homelessness

District of Columbia
Homeless Management Information System

Policies and Standard Operating Procedures

Version 5.0

Effective Date
November 1, 2015

DC HMIS Standard Operating Procedures
Table of Contents

Summary of Policies and Procedures
For Users

Policy	Procedure	Section Reference for Description
User Licenses: All users must sign a license agreement before accessing the DC HMIS.	The Agency Administrator must give each user a copy of the DC Standard Operating Procedures (SOPs) and ensure that the user has been properly trained in both the SOPs and the DC HMIS software before a user license is provided. A copy of the user license should be kept on file at the agency and faxed to the Partnership at (202) 543-5653. The Agency Administrator is required to revoke the user license and access of any user immediately upon termination of employment.	User access Levels: Section A.4 Ethical Use of Data and user agreements: Section A.9 User Licenses: Section C.2
Communication: Users are responsible for communicating any and all problems or concerns about the DC HMIS to his/her Agency Administrator.	TCP requires that each agency designate a staff person to act as the "Agency Administrator." The Agency Administrator, who receives special training, should receive questions from his/her users. When a question cannot be answered by the agency administrator, he/she may call upon the HMIS System Administrator. Communication from the HMIS System Administrator to agencies is done through the Agency Administrator, who should filter pertinent information down to front-line users.	Communication: Sections A.5 and A.6
Data Sharing: There is currently no inter-agency data sharing in the DC HMIS.	No electronic data sharing between agencies is permitted within the DC HMIS at this time. Programs within agencies may share data as decided upon by the agency's executive director and/or agency administrator. Users may not change default client record security settings to "open." Users that are found to be inappropriately opening client records to other agencies will have their access to the DC HMIS immediately terminated.	Data Sharing: Section A.8 Profile Information: Section D.6

Policy	Procedure	Section Reference for Description
Client Rights, Consent, and Ethical Use of Data: Each agency and user must abide by the terms of the agency privacy policy, the DC HMIS SOPs and the Terms and Conditions of ServicePoint.	Personal information collected about the persons served within programs should be protected. Misuse of this data can result in termination of access to the DC HMIS or personnel action by the agency. Each agency must have a privacy posting at the point of intake for review by consumers. The DC HMIS operates under a model of inferred consent, which means that permission to enter a consumer's information into the HMIS is inferred when a notice is posted and he/she accepts the services offered. Consumer refusal to provide information or otherwise participate in HMIS shall not be reason to deny eligibility or services.	Ethical Use of Data/Client Rights and Consent: A.9 and A.11 Inferred Client Consent: D.2.
Data Removal, Review and Grievances: A consumer may request to see their HMIS data or may request that personally identifying information be removed from the HMIS.	Consumers may follow the Agency's grievance policy on issues related to HMIS. Grievances related to HMIS that cannot be addressed at the agency level may be escalated in writing to the Community Partnership. In response to a legitimate request from a consumer to remove his/her personally identifying information from the HMIS, the agency should remove such data from the client record within 72 hours. A record of these transactions must be kept by the Agency Administrator. In response to requests to view his/her data in the HMIS, the agency administrator or case manager must provide a copy of the requested data within a reasonable time frame to the consumer. Requests for changes to client information are considered on a case by case basis.	Client Grievances: A.13 Data Retrieval, Client: Section D.12
Security and User Access: Each user is provided with a unique user name and password.	Sharing of user names and passwords is prohibited in the DC HMIS. Sharing of user name/passwords is considered a serious breach of the user agreement and could result in sanctions and/or appropriate personnel action.	Security: Section B.1

Policy	Procedure	Section Reference for Description
Security and Data Retrieval: Agencies must protect identified data that is downloaded or retrieved from the HMIS onto local computers and/or networks.	Once identified data has been retrieved from the HMIS and saved to a PC, network or disk, the data must be kept secure through encryption and/or password protection. Storing identified data on floppy disks, CDs, flash drives or unprotected laptops is not recommended unless proper security precautions have been taken. Unencrypted or unprotected data from the HMIS may not be sent via email.	Extracted Data: Section B.5
Security Requirements for Agencies: Because the DC HMIS is accessed over the internet and contains personal data that must be protected, each agency is required to follow a minimum set of guidelines to ensure security of the entire system.	Each agency must have the following protections in place on the network or stand-alone PC that accesses the DC HMIS: Physical space of the computer must be protected to prevent unauthorized access; Use of non-agency computers (internet cafes, library) is prohibited; Time-out routines must be enabled on computers accessing the HMIS; Each computer that is on the network must have current virus protection software that updates automatically; Each network or computer must have a hardware or software firewall installed and active.	Data Access Computer Requirements: B.6
Training: The Partnership provides user training on a variety of HMIS topics.	Although initial user training may be conducted by the Agency Administrator, the Partnership offers a schedule of user training on a monthly basis in a classroom style setting. The schedule for these trainings is available on TCP's web site.	Training: Section C.5 and **www.community-partnership.org**.

Policy	Procedure	Section Reference for Description
Data Collection and Data Quality: Each program is required to collect a series of data elements depending on the type of program it operates. The Partnership's data elements are largely based on HUD's Data and Technical Standards. Data entry must meet the Partnership's data quality thresholds to be considered complete.	Each CoC program must have all the required data elements in the DC HMIS weekly. Data entry for the previous week must be completed on the following Monday. Special provisions may be made for domestic violence programs. Data quality and integrity is expected of HMIS users. The Partnership may perform data quality reviews and require corrective action if data quality does not meet threshold review.	Required Data Collection: Section D.1. Specific data elements by program type are detailed in Attachment H. Data Integrity: Sections d.9, D.10 and D11

The Community Partnership
District of Columbia Homeless Management Information System
(DC HMIS)

Policies and Standard Operating Procedures

This document details the policies, procedures, guidelines, and standards that govern the operations of the D.C. Homeless Management Information System (DC HMIS). It outlines the roles and responsibilities of all agencies and persons with access to DC HMIS data, and it contains important and useful information about the ways in which DC HMIS data is secured and protected. All Providers using the DC HMIS should read this document in full and train every end user within its agency and programs to understand its contents as necessary. Attachment A is a user license agreement, which includes a statement that the user has read and understands these operating procedures.

Introduction:

The Community Partnership (TCP) is a non-profit corporation under contract with the D.C. Department of Human Services (DHS) and the U.S. Department of Housing and Urban Development (HUD) to manage public homeless services in the District of Columbia. In order to accomplish this work, TCP subcontracts for the direct provision of services to local providers.

DHS and HUD require TCP to provide unduplicated statistical demographic reports on the numbers and characteristics of clients served as well as on program outcomes. In order to address the reporting requirements mandated by DHS and HUD, TCP has implemented an electronic management information system that will provide the necessary demographic information and reports. This system is called the D.C. Homeless Management Information System (DC HMIS). Bowman Internet Systems is the vendor of the web-based software known as *ServicePoint,* which was selected by TCP in consultation with local service providers in 2000 as part of a competitive process. TCP provides or arranges for training and technical assistance to users of the DC HMIS. All Providers funded by DHS or that receive certain HUD grants (Supportive Housing Program, Shelter Plus Care, Emergency Shelter Grants, Homeless Prevention and Rapid Re-housing Program) are required to participate in the DC HMIS. Some privately funded providers participate on a voluntary basis.

Providers participating in the DC HMIS are required to collect and record certain data elements for all new and continuing clients in the HMIS (see Attachment B for a description of the universal and program-specific data elements required by program type) weekly. Data entry should be completed weekly for all providers. All records should be up to date every Monday for clients served during the prior week. All Providers using the DC HMIS are also required

to comply with HUD's *HMIS Data and Technical Standards* (see Attachment C for an overview and a full copy of the Standards).

TCP recognizes the importance of maintaining confidential client records in a secure environment to ensure that the information is not misused or accessed by unauthorized people. The following Policies and Standard Operating Procedures (SOP) have been developed to establish standards for the collection, storage and dissemination of confidential information by the users of the DC HMIS. TCP has developed a privacy policy regarding the use and disclosure of data in the HMIS and by programs operated directly by TCP (see Attachment D for a copy of this policy).

The DC HMIS is operated primarily as a closed system. The DC HMIS does not currently allow for sharing of electronic data between agencies, unless otherwise stated in this document. Programs can share information through other methods unrelated to the DC HMIS, as outlined in their specific program policies. TCP is the System Administrator for the DC HMIS and as such is the only entity able to access all the client-level information, including personal identifiers, contained in the DC HMIS. Acceptable uses and disclosures of the data are outlined in TCP's privacy policy. For example, TCP may disclose data that is required under a court order issued by a judge, to protect the health and safety of those being served in its programs, and may use de-identified data for research and analysis purposes. TCP does not provide access to client-level data containing personal identifiers to any agency. Although DHS has the authority to view the data in the DC HMIS related to programs it funds, it has agreed to relinquish the right to view client level data. Additionally, HUD does not require any client-level information from the DC HMIS for the programs it funds. Thus only de-identified and/or aggregate-level data is shared with DHS and HUD.

TCP's HMIS Goals:

The goals of the DC HMIS are to support and improve the delivery of homeless services in the District of Columbia. Inclusive in these goals is the improvement of the knowledge base about homelessness that contributes to an enlightened and effective public response to homelessness. The DC HMIS is a tool that facilitates the following:

- *Improvements in service delivery* for clients as case managers assess the client's needs, inform the client about available services on site or through referral, help the client find and keep permanent housing, and improve service coordination when information is shared between programs within one agency that are serving the same client.
- *A confidential and secure environment* that protects the collection and use of all client data including personal identifiers.
- The *automatic generation of standard reports* required by HUD or DHS, including the District's participation in the national Annual Homelessness Assessment Report (AHAR).

- *Generation of system-level data* and analysis of resources, service delivery needs and program outcomes for the District's homeless population.
- A *data collection and management* tool for Authorized Agencies to administer and supervise their programs.

TCP recognizes the need to maintain each client's confidentiality, and will treat the personal data contained within the DC HMIS with respect and care. As the guardians entrusted with this personal data, TCP has both an ethical and a legal obligation to ensure that data is collected, accessed and used appropriately. Of primary concern to TCP are issues of security (i.e. encryption of data traveling over the Internet, the physical security of the HMIS server), and the policies governing the release of this information to the public, government and funders.

Meeting the needs of homeless persons served by TCP and its Providers is the underlying and most basic reason for having the DC HMIS, and employing it for continued improvements in program quality.

Definitions

Many of the terms used in this Policies and Standard Operating Procedures Manual may be new to many users. Definitions of some of these terms are as follows:

Agency Administrator: The person responsible for system administration at the agency level. This person is responsible for adding and deleting users, basic trouble-shooting, introductory training of agency users and organizational contact with the DC HMIS System Administrator.

Authentication: The process of identifying a user in order to grant access to a system or resource; usually based on a username and password.

Authorized Agency: Any agency, organization or group who has an HMIS Agency Agreement and/or contract with The Community Partnership and that is allowed access to the DC HMIS database. These Agencies connect independently to the database via the Internet.

Bowman Internet Systems: Also known as Bowman. The company that wrote the software used for the DC HMIS. Bowman Internet Systems also houses and maintains the server owned by The Community Partnership that holds our HMIS database.

Client: Any recipient of services offered by a Provider or Authorized Agency.

Client-level Data: Data collected or maintained about a specific person. This type of data can be de-identified for purposes of data analysis, which means that personally identifying information is removed from the record.

Community Agency: Agencies participating in the DC HMIS that are not currently receiving funding from The Community Partnership.

DC HMIS: The specific HMIS utilized in the District of Columbia. Currently the DC HMIS uses software produced by Bowman Internet Systems, called *ServicePoint*.

DC HMIS System Administrator: The job title of the person at The Community Partnership who provides technical support and training to HMIS users. This person has the highest level of user access in ServicePoint and has full access to all user and administrative functions.

Database: An electronic system for organizing data so it can easily be searched and retrieved; usually organized by fields and records.

De-identified Data: Data that has been stripped of personally identifying information.

Encryption: Translation of data from plain text to a coded format. Only those with the "key" have the ability to correctly read the data. Encryption is used to protect data as it moves over the internet and at the database level through the use of special software.

Firewall: A method of controlling access to a private network, to provide security of data. Firewalls can use software, hardware, or a combination of both to control access.

HMIS: Homeless Management Information System. This is a generic term for any system used to manage data about homelessness and housing.

HUD HMIS Data and Technical Standards (the Standards): Standards HUD published in the Date Register No. and Volume need to be updated. These standards fall into three categories: a) data elements required to be collected by HMIS users including "universal" and "program specific" data elements; b) Privacy and Security Standards for data confidentiality; and c) Technical Standards for the creation of HMIS data systems.

Identifying Information: Information that is unique to an individual and that may be used to identify a specific person. Examples of identifying information are name and social security number.

Module: The ServicePoint software has several sections that focus on different types of functions related to HMIS. These sections, known as "modules," include ClientPoint (for entering client data), ResourcePoint (for looking up homeless services), and ShelterPoint (for checking clients in and out of beds). Modules may be added to the DC HMIS as needed in the future.

Chief of Policy and Programs: This position at TCP is responsible, among other duties, for managing the HMIS project including overseeing data collection methods and quality assurance practices to ensure the reliability of TCP research on program operations and outcomes.

Provider: Shall mean any organization under contract with TCP to provide outreach, shelter, housing, employment and/or social services to homeless people.

Server: A computer on a network that manages resources for use by other computers in the network. For example, a file server stores files that other computers (with appropriate permissions) can access. One file server can "serve" many files to many client computers. A database server stores a data file and performs database queries for client computers.

***ServicePoint*:** A web-based software package developed by Bowman Internet Systems which tracks data about people in housing crisis in order to determine individual needs and provide aggregate data for reporting and planning.

TCP: The Community Partnership. The Community Partnership is an intermediary funding and planning organization in District of Columbia, with the goal of eliminating homelessness in the District of Columbia. The Community Partnership manages the HMIS for the District of Columbia.

User: An individual who uses a particular software package; in the case of the DC HMIS, the *ServicePoint* software.

User License: An agreement with a software company that allows an individual to use the product. In the case of ServicePoint, user licenses are agreements between The Community Partnership and Bowman Internet Systems that govern individual connections to the DC HMIS. User licenses cannot be shared.

A. Organization and Management of the DC HMIS

A.1. Project Management

Policy: The Community Partnership is responsible for project management and coordination of the DC HMIS. TCP employs an HMIS team who is responsible for all system-wide policies, procedures, communication, performance measurement reporting and coordination. The HMIS team is the primary contact with Bowman Internet Systems and works with Bowman to implement any necessary or desired system-wide changes and updates. In this role as Project Manager, TCP endeavors to provide a uniform DC HMIS that yields the most consistent data for client management, agency reporting and service planning.

Procedure: All concerns relating to the policies and procedures of the HMIS should be addressed with TCP's Chief of Policy and Programs; however, the Executive Director of TCP is the final authority for policies and procedures of the DC HMIS.

A.2. DC HMIS System Administrator

Policy: TCP employs an HMIS Coordinator (who is a member of the HMIS team) whose primary responsibility is the coordination and administration of the DC HMIS. In the absence of the HMIS Coordinator, TCP's Research Associate (also a member of the HMIS Team) designates a backup staff member for responding to Authorized Agencies or develops a contingency plan for doing so.

Procedure: The DC HMIS Coordinator manages day-to-day operations of the DC HMIS and is governed by a TCP confidentially agreement that allows access to client level data. The confidentiality agreement is available for public review upon request.

All system-wide questions and issues should be directed to the DC HMIS System Administrator. TCP's Executive Director is ultimately responsible for all final decisions regarding planning and implementation of the DC HMIS.

A.3. Agency Administrators

Policy: Each Authorized Agency must designate a staff member to be the HMIS Agency Administrator who is responsible on a day-to-day basis for enforcing the data and office security requirements under these Policies and Standard Operating Procedures.

Procedure: The Executive Director of the Authorized Agency must identify an appropriate Agency Administrator and provide that person's name, qualifying skills and contact information to the DC HMIS System Administrator. Changes to that information over time should be reported immediately to the DC HMIS System Administrator. The DC HMIS System Administrator is responsible for maintaining a current list of Agency Administrators.

Agency Administrators are responsible for the following:

- Serves as the primary contact between the Authorized Agency and TCP.
- Must have an email address and be a licensed user.
- Manages agency user licenses; adding and removing licensed users for their agency; Agency Administrators are required to remove licensed users from the HMIS immediately upon termination from agency, placement on disciplinary

probation, or upon any change in duties not necessitating access to HMIS information. All changes must be relayed to the DC HMIS System Administrator.

- Must be technically proficient with a web-based MIS since he/she will be responsible for maintaining the Authorized Agency's HMIS site.
- Has access to all client data, user data and agency administration information for the Authorized Agency; thus is responsible for the quality and accuracy of these data.
- Ensures the stability of the agency connection to the Internet and *ServicePoint*, either directly or in communication with other technical professionals.
- Trains agency end users; this includes training all Authorized Agency staff on how to use *ServicePoint* as well as training to ensure compliance with privacy and security policies.
- Provides support for the generation of agency reports.
- Monitors and enforces compliance with standards of client confidentiality and ethical data collection, entry, and retrieval at the agency level.

A.4. User Access Levels

Policy: All DC HMIS Users will have a level of access to HMIS data that is appropriate to the duties of their position so that information is recorded and accessed on a "need to know" basis. All users should have the level of access that allows efficient job performance without compromising the security of the DC HMIS or the integrity of client information.

Explanation: The DC HMIS provides appropriate and layered levels of access to ensure the security of HMIS data. *ServicePoint* allows multiple levels of user access to data contained in the database. Access is assigned when new users are added to the system and can be altered as needs change. The ability to change user access levels allows for legitimate changes in agency needs and removes the temptation to share logins in order to by-pass access restrictions. In the interest of client data security, the Agency Administrator will always attempt to assign the most restrictive access that allows efficient job performance.

Procedure: Each Agency Administrator (and/or its Executive Director) will identify the level of access each licensed user will have to the HMIS database. Levels of access are detailed below.

User Levels: There are several levels of access to *ServicePoint*. These levels should be reflective of the access a user has to client level paper records and should be determined by a staff person's position in the organization, their direct interaction with clients and their data entry responsibilities. ServicePoint access levels are described in the table below.

Resource Specialist I	Access is limited to the *ResourcePoint* module. This role allows the User to search the database of area agencies and programs and view the detail screens for each agency or program. Access to client or service records is not given. A Resource Specialist cannot modify or delete data.
Resource Specialist II	The same access rights as Resource Specialist I, however, this person is considered an agency-level I&R Specialist who updates their own agency and program information.
Resource Specialist III	The same access rights as Resource Specialist II, however, this person is a system-wide I&R Specialist who can update any agency or program information. This access level can also edit the system-wide news.
Volunteer	A volunteer can view or edit basic demographic information about clients (the profile screen), but is restricted from viewing detailed assessments. A volunteer can enter new client records, make referrals, or check-in/out a client from a shelter. Normally, Administrators assign this User Access Level to individuals who complete client intake and then refer the client to an Agency Staff User or a Case Manager.
Agency Staff	Agency staff has access to *ResourcePoint*, limited access to *ClientPoint*, full access to service records and access to most functions in *ServicePoint*. However, Agency Staff can only access basic demographic data on clients (profile screen). All other screens are restricted, including assessments and case plan records. They have full access to service records. Agency Staff can also add news items to the *Newsflash* feature. There is no reporting access.
Case Manager	Case Managers have access to all features excluding administrative functions. They have access to all screens within *ClientPoint*, including the assessments and full access to service records. There is full reporting access with the exception of audit reports.
Agency Administrator	Agency Administrators have access to all features, including agency level administrative functions. This level can add/remove Users for his/her agency and edit their agency and program data. They have full reporting access. They cannot access the following administrative functions: Assessment

	Administration, Picklist Data, Licenses, Shadow Mode, or System Preferences.
Executive Director	Same access rights as Agency Administrator, but ranked above Agency Administrator. Has the ability to delete Agency Administrator accounts.
System Operators	System Operators have no access to *ClientPoint* or *ShelterPoint*. They have no access to reporting functions, but do have access to administrative functions. The System Operator can setup new agencies, add new Users, reset passwords, and access other system-level options. The System Operator helps to maintain the system, but does not have access to any Client or Service Records. The System Operator can order additional User Licenses and modify the allocations of Licenses.
System Administrator I	Same access rights to client information (full access) as Agency Administrator. However, this User has full access to administrative functions.
System Administrator II	System Administrator IIs have full and complete access to the system. However, this User does not have the option of choosing a Provider other than the default Provider assigned to their ID.

A.5. TCP Communication with Authorized Agencies

Policy: The DC HMIS Coordinator **is responsible for relevant and timely communication with each agency regarding the DC HMIS. The DC HMIS System Administrator will communicate system-wide changes and other relevant information to Agencies as needed. He/she will also maintain a high level of availability to Authorized Agencies.**

Explanation: Good communication is essential to the proper functioning of any system, electronic or otherwise. Providing a single point of communication simplifies and speeds communications within the DC HMIS. The DC HMIS Coordinator will also develop and maintain a listserv to facilitate communication with agency administrators, who will be required to sign up for the listserv.

Procedure: General communications from the DC HMIS System Administrator will be directed towards the Agency Administrator. Specific communications will be addressed to the person or people involved. The DC HMIS System Administrator will be available via email, phone, and mail. While specific problem resolution may take longer, the DC HMIS System Administrator will strive to respond to Authorized Agency questions

and issues within three business days of receipt. In the event of planned unavailability, the DC HMIS System Administrator will notify Authorized Agencies in advance and designate a backup contact. Information affecting all users will be directed to the Agency Administrators. Agency Administrators are responsible for distributing that information to any additional people at their agency who may need to receive it, including, but not limited to, Executive Directors, client intake workers, and data entry staff. Agency Administrators are responsible for communication with all of their agency's users.

A.6. Authorized Agency Communication with TCP

Policy: Authorized Agencies are responsible for communicating needs and questions regarding the DC HMIS directly to the DC HMIS Coordinator. In order to foster clarity both for DC HMIS users and for Bowman Internet Systems, ALL communications with Bowman regarding the DC HMIS must go through the DC HMIS Coordinator.

Explanation: TCP holds the contract with Bowman, and is therefore responsible for acting as the primary contact for the DC HMIS. Designated points of communication within Authorized Agencies and within TCP simplify and speed communications about the DC HMIS.

Procedure: Users at Authorized Agencies will communicate needs, issues and questions to the Agency Administrator. If the Agency Administrator is unable to resolve the issue, the Agency Administrator will contact the DC HMIS System Administrator via email, phone or mail. The DC HMIS System Administrator will attempt to respond to Authorized Agency needs within three business days of the first contact. If the DC HMIS System Administrator cannot resolve the issue, he/she may contact Bowman Internet Systems for technical assistance. If Agency Administrators desire to escalate any HMIS issues beyond the DC HMIS System Administrator, they should contact TCP's Chief of Policy and Programs directly via phone, email or mail. Should an HMIS issue require additional attention, an Agency Administrator may contact TCP's Executive Director in writing.

A.7. System Availability

Policy: **TCP and Bowman Internet Systems will provide a highly available database server and will inform users in advance of any planned interruption in service.**

Explanation: A highly available database affords agencies the opportunity to plan data entry, management, and reporting according to their own internal schedules. Availability is the key element in maintaining an HMIS that is a useful tool for Authorized Agencies to use in managing programs and services.

Procedure: No computer system achieves 100% uptime. Downtime may be experienced for routine maintenance, in the event of a disaster or due to systems failures beyond the control of Bowman Internet Systems or TCP. In the event of disaster or routine planned server downtime, Bowman Internet Systems will contact the DC HMIS System Administrator. The DC HMIS System Administrator will contact Agency Administrators and inform them of the cause and duration of the interruption in service. The DC HMIS System Administrator will log all downtime for purposes of system evaluation. In the event that it is needed, Bowman Internet Systems is required to have redundant systems in place so that connection to the server can be restored as quickly as possible.

A.8. Inter-Agency Data Sharing

Policy: In accordance with the Privacy Policy, Inter-Agency data sharing shall be limited to only what is necessary to provide clients with services i.e. the Coordinated Assessment and Housing Program.

Explanation: The need for client confidentiality and the benefit of integrated case management should be balanced when discussing inter-agency data sharing. During the HMIS planning process (conducted in 2000), providers were not in favor of electronic data sharing within the HMIS. These Standard Operating Procedures may be amended in the future to include data sharing between Authorized Agencies and to state explicitly how data may be shared if the community of users/providers supports that change as is the case with the Coordinated Assessment and Housing Program.

Procedure: When new clients and new service records are entered into ServicePoint, the initiating user must maintain the default setting of each record as “closed” to users from other Authorized Agencies. Closed sections of the record can neither be seen nor changed by users from other Authorized Agencies.

A.9. Ethical Data Use

Policy: Data contained in the DC HMIS will only be used to support or report on the delivery of homeless and housing services in the District of Columbia. Each HMIS User will affirm the principles of ethical data use and client confidentiality

contained in the DC HMIS Policies and Standard Operating Procedures Manual and the HMIS User Agreement. Each Authorized Agency must have a written privacy policy that includes policies related to employee misconduct or violation of client confidentiality. All HMIS Users must understand their Agency's privacy policy, and a signed policy statement must become a permanent part of the employee's personnel file.

Explanation: The data collected in the DC HMIS is the personal information of people in the District of Columbia community who are experiencing a housing crisis. It is the user's responsibility as the guardian of that data to ensure that it is only used to the ends to which it was collected and in and the manner to which the individual client has given consent.

Procedure: All HMIS users will sign an HMIS User Agreement before being given access to the DC HMIS. Any individual or Authorized Agency misusing, or attempting to misuse HMIS data will be denied access to the database, and his/her/its relationship TCP or the DC HMIS may be terminated.

A.10. Access to Core Database

Policy: No one but TCP (or its designee) and/or Bowman Internet Systems will have direct access to the DC HMIS database through any means other than the *ServicePoint* software, unless explicitly given permission by TCP during a process of software upgrade, conversion or for technical assistance.

Explanation: This policy prevents a user from accessing the HMIS database and viewing its contents, thus rendering the security measures within *ServicePoint* ineffectual.

Procedure: Under its contract with TCP, Bowman Internet Systems will monitor both our web application server and our database server and employ updated security methods to prevent unauthorized database access. Also, any party who has access to the DC HMIS database (including Bowman) must sign a Health Insurance Portability and Accountability Act (HIPAA)-compliant confidentiality agreement prior to system access.

A.11. Client Rights and Confidentiality of Records

Policy: The DC HMIS System operates under a protocol of *inferred consent* to include client data in the HMIS. Each Authorized Agency is required to post a sign about their privacy policy in a place where clients may easily view it (at the point of intake, on a clipboard for outreach providers, in a case management

office). The privacy posting should include a statement about the uses and disclosures of client data as outlined in this document. Written authorization for inclusion of a client's data in HMIS is not required, but is inferred when a client accepts the services offered by the program and when the privacy posting is displayed for client review.

Clients may opt out of HMIS or be unable to provide basic personal information. Clients have the right of refusal to provide personal identifying information to the HMIS, except in cases where such information is required to determine program eligibility or is required by the program's funders. Such refusal or inability to produce the information shall not be a reason to deny eligibility or services to a client. When a client exercises his/her right of refusal, de-identified demographic (anonymous) information will be entered into the HMIS.

Each Authorized Agency shall take appropriate steps to ensure that authorized users only gain access to confidential information on a "need-to-know" basis in accordance with TCP's Privacy Policy. Duly authorized representatives of TCP and DHS (for DHS-funded programs) may inspect client records (including electronic records) at any time as allowed under the District of Columbia Homeless Services Reform Act, although by mutual agreement, DHS will not as a matter of routine be accessing protected private information. TCP and Authorized Agencies will ensure the confidentiality of all client data as described in this document.

Explanation: The data in the DC HMIS is personal data, collected from people in a vulnerable situation. TCP and Authorized Agencies are ethically and legally responsible to protect the confidentiality of this information. The DC HMIS will be a confidential and secure environment protecting the collection and use of client data.

Procedure: Access to client data will be controlled using security technology and restrictive access policies. Each Authorized Agency (including TCP) must develop and make available a privacy policy related to client data captured in HMIS and through other means. A posting that summarizes the privacy policy must be placed in an area easily viewed by clients, and must also be placed on the Authorized Agency's web site (if they have one). Only individuals authorized to view or edit individual client data in accordance with the stated privacy policies and these Standard Operating Procedures will have access to that data. The DC HMIS will employ a variety of technical and procedural methods to ensure that only authorized individuals have access to individual client data.

A.12. Authorized Agency Grievances

Policy: Authorized Agencies will contact the DC HMIS System Administrator to resolve HMIS problems including but not limited to operation or policy issues. If

an issue needs to be escalated, Authorized Agencies may contact TCP's Chief of Policy and Programs. TCP's Executive Director will have final decision-making authority over all grievances that arise pertaining to the use, administration and operation of the DC HMIS.

Explanation: In order for the DC HMIS to serve as an adequate tool for Authorized Agencies and guide for system-wide planning, any HMIS problems must be addressed by the organization with the means to affect system-wide change. Because many agencies with varied funding streams and applicable laws participate in the HMIS, TCP's Executive Director (rather than DHS or HUD) is the appropriate party for resolution of sensitive issues that must be escalated beyond the HMIS System Administrator.

Procedure: Authorized Agencies will bring HMIS problems or concerns to the attention of the DC HMIS **System** Administrator, who may ask for these issues to be stated in writing. If problems, concerns or grievances cannot be resolved by the DC HMIS **System** Administrator, or if it is not appropriate to raise the issue with the DC HMIS **System Administrator**, the issue will be directly relayed to TCP's Chief of Policy and Programs via phone, email or mail. If the grievance requires further attention, TCP's Executive Director shall have final decision-making authority in all matters regarding the DC HMIS.

A.13. Client Grievance

Policy: Clients must contact the Authorized Agency with which they have a grievance for resolution of HMIS problems. Authorized Agencies will report all HMIS-related client grievances to TCP. If the Authorized Agency's grievance process has been followed without resolution, the Authorized Agency may escalate the grievance to TCP as outlined in Section A.12. At any time, clients may request that their personally-identifying information be removed from the DC HMIS.

Explanation: A clear and effective client grievance policy protects the needs of the client and the confidentiality of client data.

Procedure: Each Authorized Agency is responsible for answering questions, complaints, and issues from their own clients regarding the DC HMIS. Authorized Agencies will provide a copy of their privacy policy and/or of the DC HMIS Policies and Standard Operating Procedures Manual upon client request. Client complaints should be handled in accordance with the Authorized Agency's internal grievance procedure, and then escalated to TCP in writing if no resolution is reached.

TCP is responsible for the overall use of the HMIS, and will respond if users or Authorized Agencies fail to follow the terms of the HMIS agency agreements, breach

client confidentiality, or misuse client data. Authorized Agencies are obligated to report all HMIS-related client problems and complaints to TCP, which will determine the need for further action. The DC HMIS System Administrator will record all grievances and will report these complaints to the Chief of Policy and Programs. Resulting actions might include further investigation of incidents, clarification or review of policies, or sanctioning of users and Agencies if users or Agencies are found to have violated standards set forth in HMIS Agency Agreements or the Policies and Standard Operating Procedures Manual.

Upon the client's request for data removal from the DC HMIS, the Agency Administrator will delete all personal identifiers of client data within 72 hours. A record of these transactions will be kept by the Agency Administrator.

A.14. Authorized Agency Hardware/Software Requirements

Policy: When possible and as funds permit, TCP will assist Authorized Agencies in obtaining computers and Internet access for the DC HMIS. If TCP is unable to assist in this task Authorized Agencies will provide their own computer and method of connecting to the Internet, and thus to the DC HMIS.

Explanation: The Community Partnership understands the cost and difficulty of acquiring and maintaining computers and Internet access. TCP may be able to assist in these costs, but funds are limited.

Procedure: Contact the DC HMIS System Administrator for the current status of assistance.

Hardware/Software Requirements: ServicePoint is web-enabled software; all that is required to use the database is a computer, a valid username and password, and the ability to connect to the Internet using internet browser software (Internet Explorer, Google Chrome, Firefox, etc.). There is no unusual hardware or additional ServicePoint-related software or software installation required. Bowman guidelines state the following minimum and recommended workstation specifications.

Minimum Workstation Requirements

Computer: PC 500 MHz or better

Web Browser (newest version of the following): Microsoft Internet Explorer, Google Chrome, Mozilla Firefox, or Apple Safari

Hard Drive: 2
GB 64 MB RAM

Internet Connectivity (broadband or high-speed)
SVGA monitor with 800 x 600+ resolution

Keyboard and Mouse

Recommended Workstation Requirements

Computer: 1 GHz Pentium Processor PC

Web Browser (newest version of the following): Microsoft Internet Explorer, Google Chrome, Mozilla Firefox, or Apple Safari

20 GB Hard Drive

256 MB RAM

Broadband Internet Connection - 128 kpbs (hosted version) or LAN connection

SVGA monitor with 800x600 + resolution

Keyboard and mouse

Although there is no unusual hardware or additional ServicePoint-related software required to connect to the database, the speed and quality of the Internet connection and the speed of the hardware and could have a profound effect on the ease of data entry and report extraction. A high-speed Internet connection, like a DSL or ISDN line with speeds at or above 128.8 Kbps, is preferred, as is a computer with speeds above 166MHz. Bowman also recommends the use of Windows 7 (1 GHz models or faster) as the Windows platform to eliminate certain technical problems.

A.15. Authorized Agency Technical Support Assistance

Policy: The Community Partnership will provide technical assistance including ongoing software support for users of the DC HMIS. Internal hardware and internet connectivity issues should be addressed by the Authorized Agency's internal IT staff to the extent possible.

Explanation: Even though the equipment and internet connection used to connect to the DC HMIS is owned by the Authorized Agency, TCP will provide technical assistance when possible and as resources allow.

Procedure: Hardware and connectivity issues not related to the HMIS software should be addressed by the Authorized Agency's internal IT staff. Authorized Agencies may contact the DC HMIS System Administrator for technical support of the components necessary to connect to the DC HMIS.

A.16. Users' Guide

Policy: TCP will provide a DC HMIS Users' Guide and Data Dictionary for all DC HMIS Users. The User's Guide and other documentation will be posted in the HMIS section of TCP's web site located at www.community-partnership.org.

Explanation: An internal users' guide and Data Dictionary provides software users with information about how the software product is used in a particular community. The DC HMIS Users' Guide will provide specific technical instruction to DC HMIS Users about how to use ServicePoint.

Procedure: The DC HMIS System Administrator will create, distribute and update the DC HMIS Users' Guide and Data Dictionary. These will include procedures that are held in common for all Authorized Agencies, and forms for customizing the Users' Guide for each Authorized Agency. The guide template and data dictionary will be provided to all users during user training and will be made available on TCP's web site.

A.17. Monitoring and Evaluation

Policy: TCP will regularly monitor and evaluate the effectiveness of the DC HMIS and, based on the information received, will continue to make enhancements to the DC HMIS and the Policies and Standard Operating Procedures as necessary.

TCP will also include HMIS in its standard contractor monitoring protocol. This may include compliance with the HMIS Standard Operating Procedures and with HUD's Data and Technical Standards.

Explanation: Monitoring and evaluation helps ensure security and proper usage of the DC HMIS.

Procedure: The DC HMIS System Administrator will conduct internal system monitoring and may contact Agency Administrators to schedule monitoring and evaluation visits. TCP's monitoring staff may also contact Agency Administrators or other Authorized Agency staff in relation to the HMIS portion of standard monitoring visits conducted by TCP over the course of each year.

B. Security and Access

B.1. User Access

Policy: Agency Administrators will provide unique user names and initial passwords to each Authorized Agency user. User names will be unique for each user and will not be exchanged or shared with other users. The DC HMIS System Administrator will have access to the list of user names for the DC HMIS and will track user name distribution and use. Only TCP will be authorized to purchase or grant additional user licenses to an Agency that has utilized all current licenses.

Explanation: Unique user names and passwords are the most basic building block of data security. Not only is each user name assigned a specific access level, but in order to provide to clients or program management an accurate record of who has altered a client record, when it was altered, and what the changes were (called an "audit trail") it is necessary to log a user name with every change. Exchanging or sharing user names seriously compromises the security of the DC HMIS, and will be considered a breach of the user agreement and will trigger appropriate repercussions and/or sanctions for the user and agency.

Procedure: Agency Administrators will provide unique user names and initial passwords to each user upon completion of training and signing of a confidentiality agreement and receipt of the Policies and Standard Operating Procedures Manual. The sharing of user names will be considered a breach of the user agreement. Agency Administrators are responsible for distributing user names and initial passwords to agency users as well as for providing current users with a new password if he/she requires one.

B.2. User Changes

Policy: The Authorized Agency Administrator will make any necessary changes to the Authorized Agency user accounts. This includes issuance of new passwords, revoking authorization for staff that are no longer with the agency and managing access levels, etc.

Explanation: The Agency Administrator has the ability to change user names and re-distribute user licenses to accommodate Authorized Agency organization.

Procedure: The Agency Administrator will make any necessary changes to the list of Authorized Agency users. Changes in Agency Administrators must be reported to the DC HMIS System Administrator. The Agency Administrator is required to revoke the user license of a terminated employee immediately upon termination of employment. At the end of each month the DC HMIS Administrator will generate a report on users who have not accessed the HMIS over the prior month. The DC HMIS Administrator

will then contact the Agency Administrator and Executive Director at the respective agencies to determine whether the user license needs to be deleted. For employees with user access otherwise leaving the agency, the user license should be revoked at the end of business on the person's last day of employment.

B.3. Passwords

Policy: Users will have access to the DC HMIS via a user name and password. Passwords must be changed a minimum of once every 45 days. Users will keep passwords confidential. Under no circumstances shall a licensed user share a password nor shall they post their password in an unsecured location.

Explanation: Users will have access to the DC HMIS via a user name and password. These methods of access are unique to each user and confidential. Users are responsible for keeping their passwords confidential. For security reasons, passwords will automatically be reset every 45 days.

Procedure: The Agency Administrator will issue a user name and temporary password to each new user who has completed training. Upon sign in with the user name and temporary password, the user will be required by the software to select a unique password that will be known only to him/her. Every 45 days, passwords are reset automatically by the DC HMIS software. See Section B.1 for additional detail on password security.

B.4. Password Recovery

Policy: The Agency Administrator will reset a user's password in the event the password is lost or forgotten. Agency Administrators must validate the authenticity of the request if the request is not made in person.

Explanation: In any secure system, there is a danger that users will lose or forget their passwords.

Procedure: In the event of a lost or forgotten password, the user whose password is lost will contact the Agency Administrator. The Agency Administrator will reset the user password, and issue a temporary password to allow the user to login and choose a new password. The new password will be valid from that time forward, until the next 45-day forced change. Agency Administrators must validate the authenticity of the request if the request is not made in person. In other words, neither Agency Administrators nor the DC HMIS System Administrator shall issue a new password without ensuring that the person requesting it is, in fact, the person with the authorization to use it. For example, if a request is made by phone or email, the Agency Administrator or System

Administrator should call the user back at his/her desk (using the contact number on file) before issuing a new password.

B.5. Extracted Data

Policy: DC HMIS users will maintain the security of any client data extracted from the database and stored locally, including all data used in custom reporting. DC HMIS users will not electronically transmit any unencrypted client data across a public network.

Explanation: The custom report-writer function of ServicePoint allows client data to be downloaded to an encrypted file on the local computer. Once that file is unencrypted by the user, confidential client data is left vulnerable on the local computer, unless additional measures are taken. Such measures include restricting access to the file by adding password. For security reasons, unencrypted data may not be sent over a network that is open to the public. Unencrypted data may not be sent via email. HMIS users should apply the same standards of security to local files containing client data as to the HMIS database itself.

Procedure: Data extracted from the database and stored locally will be stored in a secure location (not on floppy disks/CDs or other temporary storage mechanisms like flash drives or on unprotected laptop computers, for example) and will not be transmitted outside of the private local area network unless it is properly protected via encryption or by adding a file-level password. The DC HMIS System Administrator will provide help in determining the appropriate handling of electronic files. All security questions will be addressed to the DC HMIS System Administrator. Breach of this security policy will be considered a violation of the user agreement, which may result in personnel action and/or agency sanctions.

B.6 Data Access Computer Requirements

Policy: Users will ensure the confidentiality of client data, following all security policies in the DC HMIS Policies and Standard Operating Procedures Manual and adhering to the standards of ethical data use, regardless of the location of the connecting computer. All Policies and Procedures and security standards will be enforced regardless of the location of the connecting computer. TCP may restrict access to the DC HMIS to specific computers in the future.

Explanation: Because ServicePoint is web-enabled software users could conceivably connect to the database from locations other than the Authorized Agency itself, using

computers other than agency-owned computers. Connecting from a non-agency location may introduce additional threats to data security, such as the ability for non-ServicePoint users to view client data on the computer screen or the introduction of a virus. If such a connection is made, the highest levels of security must be applied, and client confidentiality must still be maintained. This includes only accessing the DC HMIS via a computer that has virus protection software installed and updated.

Procedure: Each Authorized Agency and Agency Administrator is responsible for:

a) Physical Space. Authorized Agencies must take reasonable steps to insure client confidentiality when licensed users are accessing the DC HMIS. Licensed users are required to conduct data entry in a protected physical space to prevent unauthorized access to the computer monitor while confidential client information is accessible.
b) Use of a non-agency computer located in a public space (i.e. internet café, public library) to connect to HMIS is prohibited.
c) Time-Out Routines. Each Agency Administrator will be required to enable time-out (login/logout) routines on every computer to shut down access to the DC HMIS when a computer is unattended. Time-out routines will be engaged at a minimum after 10 minutes of inactivity or at other intervals as TCP determines.
d) Each computer that accesses HMIS must have current virus software that updates automatically installed.
e) If the HMIS is accessed over a network, the network must be protected by a hardware or software firewall at the server. A stand-alone machine that accesses HMIS must also have a hardware or software firewall installed and active. This may be the firewall protection included as part of the operating system or the virus protection software installed on the computer.

Questions about security of the DC HMIS should be referred to the DC System Administrator.

C. Agency Participation Requirements

C.1 DC HMIS Agency Agreements

Policy: Only Authorized Agencies will be granted licenses to access the DC HMIS system. The Community Partnership shall make the sole determination to identify Authorized Agencies. For agencies that have contracts with TCP, the agency agreement for each program is contained within the contract. For non-contracted agencies, the Executive Director will be required to sign a "HMIS Authorized Agency Agreement" (Attachment E) binding their organization to the DC HMIS Policies and Standard Operating Procedures and all applicable laws and regulations regarding the handling of client data before access is granted.

Explanation: TCP has final authority over the DC HMIS. In order to ensure the integrity and security of sensitive data, TCP will regulate access to this data. Only Agencies that have agreed to the terms set out in the HMIS Agency Agreement and or TCP Contract will be allowed access to the DC HMIS. The agency agreements will include terms and duration of access, an acknowledgement of receipt of the Policies and Standard Operating Procedures Manual, and an agreement to abide by all provisions contained therein.

Procedure: Authorized Agencies will be given a copy of the HMIS Agency Agreement or contract, the Policies and Standard Operating Procedures Manual, and any other relevant paperwork in time for adequate review and signature. Once that paperwork has been reviewed and signed by the Executive Director, the TCP HMIS System Administrator will issue a certain number of licenses for use by the agency and assist with the set-up of an Agency Administrator. Agency users will be trained to use ServicePoint by the Agency Administrator or through regular training sessions scheduled by TCP. Once training has been completed, each user will be issued a user name and password by his/her Agency Administrator.

C.2. User Licenses

Policy: In order to obtain a license, a user must successfully complete a TCP-approved training program or be trained by the Provider's Agency Administrator and must sign a User License (Attachment A) upon completing training. Sharing of licenses, User IDs or passwords is strictly prohibited. If necessary, Authorized Agencies may obtain additional User Licenses from Bowman Internet Systems through TCP. The cost for User Licenses will be determined by Bowman Internet Systems, and will not be changed by the Community Partnership.

Explanation: TCP purchases a number of user licenses on behalf of the DC Continuum of Care.

Procedure: Each Agency Administrator (or Executive Director) will identify the staff designated to be the licensed users of the DC HMIS and submit the names to the DC HMIS System Administrator. Authorized Agencies wishing to add additional users will complete a User License Agreement Form (Attachment F). The Authorized Agency will return this form to the DC HMIS System Administrator. The DC HMIS System Administrator will purchase the User Licenses from Bowman and provide a copy of the request form to the TCP Finance Department for deposit. The DC HMIS System Administrator purchases licenses online, through the ServicePoint program. The DC HMIS System Administrator will then notify the Authorized Agency when the additional Licenses are available. Bowman invoices TCP for the cost of the licenses.

C.3. User Activation

Policy: The DC HMIS Administrator is responsible for distributing licenses. The Agency Administrator will issue each new user a user name and password to access the DC HMIS upon approval by the Authorized Agency, completion of ServicePoint training, and signing of the HMIS User Agreement. Every user must receive appropriate ServicePoint training before being issued a user name and password.

Explanation: Authorized Agencies will determine which of their employees will have access to the DC HMIS. This allows for the needed flexibility in selecting users.

Procedure: The DC HMIS Administrator will distribute user licenses at the request of the Agency Administrator following the user account setup and completion of required user training. Agency Administrators will also setup user accounts and delete users as needed. Agency Administrators are responsible for notifying TCP of user changes. Agency Administrators will be responsible for training new users. TCP will provide training to Agency Administrators and will supplement this training as necessary through the regular training schedule or through on-site visits.

C.4. HMIS User Agreements

Policy: Each Authorized Agency User will sign an HMIS User Agreement before being granted access to the DC HMIS.

Explanation: Before being granted access to the DC HMIS, each user must sign an HMIS User Agreement, stating that he or she has received training, will abide by the DC HMIS Policies and Standard Operating Procedures Manual, will appropriately maintain the confidentiality of client data, and will only collect, enter and retrieve data in the DC HMIS relevant to the delivery of services to people in housing crisis in District of Columbia.

Procedure: The Authorized Agency Administrator will distribute HMIS User Agreements to new HMIS Users for signature. The user will sign the HMIS User Agreement and the agreement will be faxed or emailed to the DC HMIS System Administrator at (202) 543-5653 and for email at hmis@community-partnership.org. The Agency Administrator will also file signed HMIS User Agreements for all users. The existence of a signed HMIS User Agreement for each active user will be verified in the annual HMIS on-site review or may be checked during regular TCP monitoring of contracts. Allowing a user access to the DC HMIS without a signed user agreement is a violation of the DC HMIS Standard Operating Procedures and may result in program sanctions.

C.5. Training

Policy: The Community Partnership is responsible for defining training needs, identifying trainers and organizing training sessions for Authorized Agencies. TCP will provide various training options, to the extent possible, based on the needs of HMIS users. TCP will provide for adequate and timely ServicePoint training.

Explanation: In order for the DC HMIS to be a benefit to clients, a tool for Authorized Agencies and a guide for planners, all users must be adequately trained to collect, enter and extract data.

Procedure: TCP will provide access to training for all HMIS users. Agency Administrators will be given additional training relevant to their position. Agency Administrators will also be trained to provide basic user training for new users at their agency and will be expected to do so prior to issuing a user license to any new user. This will allow Authorized Agencies to adjust to their own staffing needs with as little interruption in database use as possible. The DC HMIS System Administrator will provide support to Agency Administrators, who will in turn provide for user training needs.

C.6. Contract Termination Initiated by Authorized Agency

Policy: Authorized Agencies that are not TCP contractors may terminate the HMIS Agency Agreement with or without cause upon 30 days written notice to TCP and according to the terms specified in the HMIS Agency Agreement. The termination of the HMIS Agency Agreement by the Authorized Agency may affect other contractual relationships with The Community Partnership and/or requirements set forth in contracts issued by HUD. In the event of termination of the HMIS Agency Agreement, all data entered into the DC HMIS will remain an active part of the DC HMIS, and records will remain closed.

Explanation: While non-TCP contracted Authorized Agencies may terminate relationships with The Community Partnership and the DC HMIS, the data entered prior to that termination would remain part of the database. This is necessary for the database to provide accurate information over time and information that can be used to guide planning for community services in District of Columbia. The termination of the HMIS Agency Agreement may affect other contractual relationships with The Community Partnership and/or HUD.

Procedure: TCP Provider Agencies are required to participate in the DC HMIS as a condition of their funding. For all non-TCP Authorized Agencies terminating the HMIS Agency Agreement, the person signing the HMIS Agency Agreement (or a person in the same position within the agency) will notify TCP's Executive Director 30 days or more from the date of termination. The Executive Director will notify the DC HMIS System Administrator. In all cases of termination of HMIS Agency Agreements, the DC HMIS System Administrator will inactivate all users from that Authorized Agency on the date of termination of agreement.

C.7. Contract Termination Initiated by The Community Partnership

Policy: The Community Partnership may terminate the HMIS Agency Agreement for non-compliance with the terms of the agreement or with the HMIS Standard Operating Procedures with written notice to the Authorized Agency. The Community Partnership may also terminate the HMIS Agency Agreement with or without cause with 15 days written notice to the Authorized Agency and according to the terms specified in the HMIS Agency Agreement. If a TCP contract is terminated under the terms of that contract, the agreement for HMIS access for that program will also be terminated. In that case, access will be renegotiated by TCP and the agency is appropriate and in accordance with these standard operating procedures. The termination of the HMIS Agency Agreement or contract by TCP may affect other contractual relationships with The Community Partnership or with HUD. In the event of termination of the HMIS Agency Agreement or TCP contract, all data entered into the DC HMIS will remain

a part of the DC HMIS and records will remain closed. If termination of the HMIS Agency Agreement or TCP contract occurs, all Authorized Agency users will be inactivated on the date the HMIS Agency Agreement or contract is terminated.

Explanation: While The Community Partnership may terminate the HMIS Agency Agreement or its contract with the Authorized Agency, the data entered by that Authorized Agency prior to termination of contract would remain part of the database. This is necessary for the database to provide accurate information over time and information that can be used to guide planning for community services in District of Columbia. The termination of the HMIS Agency Agreement may affect other contractual relationships with The Community Partnership or with HUD.

Procedure: TCP Provider Agencies are required to participate in the DC HMIS as a condition of their funding. When terminating the HMIS Agency Agreement, the Executive Director of The Community Partnership will notify the person from the Authorized Agency who signed the HMIS Agency Agreement (or a person in the same position within the agency) 15 days or more prior the date of termination of contract, unless the termination is due to non-compliance with the Standard Operating Procedures. Willful neglect or disregard of the Standard Operating Procedures may result in immediate termination of an Authorized Agency from the DC HMIS. TCP's Executive Director will also notify the DC HMIS System Administrator. In all cases of termination of HMIS Agency Agreements, the DC HMIS System Administrator will inactivate all users from that Authorized Agency on the date of termination of contract.

D. Data Collection, Quality Assurance and Reporting

D.1. Required Data Collection

Policy: Providers funded by HUD (either through TCP or directly) through the Supportive Housing Program, Shelter Plus Care, HOPWA, Section 8 Moderate Rehabilitation and the Emergency Shelter Grant are required to participate in HMIS by HUD. Other providers contracted by TCP are also required to participate in the DC HMIS. All Authorized Agencies that participate in HMIS are considered "Covered Homeless Organizations" (CHO) and are required to comply with HUD's *HMIS Data and Technical Standards* unless those standards are in conflict with local laws. This includes the collection of required data elements.

Providers shall attempt to collect basic information as detailed in Attachment G on every client served by the Provider upon intake into the Provider's facility or program. In the case of outreach, the Provider shall attempt to collect basic information outlined in Attachment G during engagement on the street. If client refuses or is unable to provide basic information, providers shall, at a minimum, enter each client as an Anonymous Entry into the DC HMIS system. Authorized Agencies may choose to collect more client information for their own case management and planning purposes.

Assessment Data Collection: Providers of certain programs (outlined in Attachment G) shall attempt to conduct detailed assessments on each client who has gone through the intake process and has been accepted into the Provider's facility or program. At a minimum, providers shall attempt to collect the assessment information required as part of HUD's Data and Technical Standards.

Timeliness of Data Entry: Providers are required to enter basic client intake data into the DC HMIS weekly. All data entry must be completed on the following Monday for clients served during the prior week.

Exceptions to these data collection policies are in place for domestic violence shelters. DV shelters should request additional instruction from the DC HMIS System Administrator.

Explanation: In order for the data contained within the DC HMIS to be useful for data analysis and reporting to funders, certain minimum data must be consistently collected throughout the system.

Procedure: Each agency should review Attachment H to determine the type of data that is required to be collected and entered into HMIS.

D.2. Client Consent

Policy: Each agency must post a sign at each intake or comparable location and on its web site (if applicable) explaining the reasons for data collection for those seeking services. Consent for entering of data into HMIS may be inferred when the proper privacy notice is posted and if the client accepts the services offered. The client has the option to opt out of allowing his or her identifying information to be added to the database. In that case, the client's data should be added to the DC HMIS without identifiers as described above, although the record should be tracked internally by the agency to minimize the number of duplicate records for one client. Electronic client data will not be shared between agencies at this time because the DC HMIS is a closed system. Client data may be shared through other means with written client consent or according to the privacy policy developed by the agency.

Explanation: Privacy Policies should be in effect for each agency to both inform clients about the uses and disclosures of their personal data and to protect the agency by establishing standard practices for the use and disclosure of data. Each client must give permission for the disclosure and/or use of any client data outside of the privacy policy developed and posted by the agency. Client consent notices must contain enough detail so that the client may make an informed decision. Clients may withdraw permission to have their personal protected information in the HMIS, or may make a request to see copies of his or her client record.

Procedure: Authorized Agencies will develop a privacy policy, which will be posted in appropriate areas for client review. TCP will review the privacy notices as part of the annual HMIS review and/or through regular monitoring. If a client denies permission to enter confidential data, the Authorized Agency will enter the de-identified data into the DC HMIS and track the record to minimize duplicate records for each client.

D.3. Client Consent Forms to Share Data

Policy: The DC HMIS does not at this time allow for the electronic sharing of data between agencies other than for the purposes of providing services such as Coordinated Entry. However, each agency should include in its privacy policy that data collected by the agency is disclosed to TCP as part of its administrative responsibility for the DC HMIS and that the data may be used for analysis and reporting purposes. TCP will only report aggregate and/or de-identified data as part of its responsibilities, and agrees to maintain the data with the highest level of confidentiality and within the security guidelines set forth in this document.

Explanation: In the HMIS planning process conducted in 2000, participating agencies agreed that electronic data sharing between agencies would not be implemented in the

District. In the event that data sharing is implemented in the future, this section of the Standard Operating Procedures will be revised as appropriate.

Procedure: Unless otherwise stated or agreed upon and with the permission of TCP's Executive Director, no electronic data sharing between agencies is currently allowed in the DC HMIS other than for the purposes of providing services such as Coordinated Entry.

D.4. Appropriate Data Collection

Policy: DC HMIS users will only collect client data relevant to the delivery of services to people in housing crises in District of Columbia and/or required by funders or by law.

Explanation: The purpose of the DC HMIS is to support the delivery of homeless and housing services in District of Columbia. The database should not be used to collect or track information not related to serving people in housing crises or otherwise required for policy development and planning purposes.

Procedure: Agency Administrators will ask the DC HMIS System Administrator for any necessary clarification of appropriate data collection. The DC HMIS System Administrator, in consultation with TCP senior management, will make decisions about the appropriateness of data being entered into the database. TCP will periodically audit pick-lists and agency-specific fields to ensure the database is being used appropriately. This concern targets data elements that can be consistently tracked and reported, and does not specifically target the contents of case management notes or other fields not to be aggregated.

D.5. Data Ownership

Policy: The DC HMIS, and any and all data stored in the DC HMIS, is the property of The Community Partnership. TCP has authority over the creation, maintenance and security of the DC HMIS. Violations of the HMIS Agency Agreement, the Standard Operating Procedures, and privacy policies developed at the agency level, or other applicable laws may subject the Authorized Agency to discipline and/or termination of access to the DC HMIS and/or to termination of other TCP contracts.

Explanation: In order to ensure the integrity and security of sensitive client confidential information and other data maintained in the database, TCP will be responsible for data ownership.

Procedure: The HMIS Agency Agreement and/or TCP contract includes terms regarding the maintenance of the confidentiality of client information, provisions regarding the duration of access, an acknowledgement of receipt of the Policies and Standard Operating Procedures Manual, and an agreement to abide by all policies and procedures related to the DC HMIS including all security provisions contained therein. Because programs participating in the DC HMIS are funded through different streams with different requirements (HUD, DHS, blended, and other), TCP shall maintain ownership of the database in its entirety in order that these funders cannot access data to which they are not legally entitled.

D.6. Data Entry Profile Information

Policy: Users will designate profile information as "CLOSED" (this is currently the default setting) in the client security portion of the profile section of a client record in ClientPoint. No user will open the profile section of a client record.

Explanation: Some users (depending on the level of access) have the ability to determine whether information in client records is "open," "closed," or "read-only" to users from other Agencies. Open sections of the record can be seen and changed by users from another agency, Closed sections of the record can neither be seen nor changed by users from another agency, and Read-Only sections of the record can be seen, but not changed by users from another agency. Because the DC HMIS is a closed system, the default setting on client records has been set to "Closed." It is a violation of these Standard Operating Procedures to open a client record to other agencies.

Procedure: Users will designate all client records as closed, as indicated in the default settings. The DC HMIS System Administrator will report any OPEN profiles and will immediately require the Agency Administrator to close these records. Repeated violation of this policy may lead to personnel action and or action against the Authorized Agency, including but not limited to immediate termination of user and/or agency access.

D.7. Data Entry: Data Element Customization

Policy: Authorized Agencies may have fields available for agency-specific customization.

Explanation: ServicePoint may include fields that can be customized on the Authorized Agency level to reflect the program-specific data collection needs of its programs. These fields are part of the ServicePoint program and are available at no additional cost.

Procedure: The DC HMIS Administrators will customize any agency-specific fields.

D.8. Data Integrity

Policy: DC HMIS users will be responsible for the accuracy of their data entry. Authorized Agency leadership will be responsible for ensuring that data entry by users is being conducted in a timely manner and will also ensure the accuracy of the data entered.

Explanation: The quality of DC HMIS data is dependent on individual users to take responsibility for the accuracy and quality of their own data entry. Agency Executive Directors and/or Agency Administrators are responsible for monitoring the quality of the data for their own program(s), since that data may be used for reporting and/or monitoring purposes. Data may also be used to measure program efficacy, which impacts funding opportunities during competitive funding processes such as the annual Continuum of Care application to HUD.

Procedure: In order to test the integrity of the data contained in the DC HMIS, the DC HMIS System Administrator will perform regular data integrity checks on the DC HMIS. The data integrity checks will include reporting of "overlaps," periodic verification of data and comparison to hard files, as well as querying for internal data consistency and null values. Any patterns of error will be reported to the Agency Administrator. When patterns of error have been discovered, users will be required to make corrections where possible, correct data entry techniques, improve the accuracy of their data entry, and will be monitored for compliance.

In addition to data quality checks performed by the DC HMIS System Administrator, each HUD-funded program is required to submit the HUD Annual Progress Report on a quarterly basis (based on the program's operating year) to the appropriate contract officer at TCP. These reports will be assessed for data quality and errors will be reported to the DC HMIS System Administrator and to the Agency Administrator. Other reports for non-HUD funded programs may also be required. TCP reserves the right to add reporting requirements if data quality appears to be decreasing or if TCP's reporting requirements change.

D.9. Quality Control: Data Integrity Expectations

Policy: Accurate and consistent data entry is essential to ensuring the usefulness of the DC HMIS. Authorized Agencies will provide acceptable levels of timeliness and accuracy. Authorized Agencies without acceptable levels of data quality or timeliness may have payments withheld or incur other contract sanctions until the problems are addressed.

Explanation: Data quality is an important aspect of the DC HMIS, and must be maintained at the agency level and by users of the system. TCP will monitor data quality as part of it HMIS management functions and as part of contract monitoring

Procedure: The DC HMIS System Administrator will perform regular data integrity checks on the DC HMIS and agencies will be required to report to TCP on a regular basis as stated in the previous section.

D.10. On-Site Review

Policy: The Community Partnership will perform annual reviews of each contracted Authorized Agency's procedures related to the DC HMIS as part of its regular monitoring. Additional monitoring may take place by TCP's contract or HMIS staff.

Explanation: Regular reviews enable The Community Partnership to monitor compliance with the Policies and Standard Operating Procedures Manual and HMIS Agency Agreements.

Procedure: The exact procedures for on-site reviews will be determined by TCP on an annual basis.

D.11. Client Data Retrieval

Policy: Any client may request to view, or obtain a printed copy of, his or her own records contained in the DC HMIS. The client will also have access to a logged audit trail of changes to those records. No client shall have access to another client's records in the DC HMIS.

Explanation: The data in the DC HMIS is the personal information of the individual client. Each client has a right to know what information about him or her exists in the database, and to know who has added, changed or viewed this information, and when these events have occurred. This information should be made available to clients within a reasonable time frame of the request.

Procedure: A client may ask his/her case manager or other agency staff to see his or her own record. The case manager, or any available staff person with DC HMIS access, will verify the client's identity and print all requested information. The case manager can also request a logged audit trail of the client's record from the Agency Administrator. The Agency Administrator will print this audit trail, give it to the case manager, who will give it to the client. The client may request changes to the record, although the agency can follow applicable law regarding whether to change information based on the client's request. A log of all such requests and their outcomes should be kept on file in the client's record.

D.12. Public Data Retrieval

Policy: The Community Partnership will address all requests for data from entities other than Authorized Agencies or clients. No individual client data will be provided to any group or individual that is neither the Authorized Agency that entered the data or the client him or herself without proper authorization or consent. TCP will provide aggregate reports for the larger community. The content of these reports will reflect a commitment to client confidentiality and ethical data use.

Explanation: Any requests for reports or information from an individual or group who has not been explicitly granted access to the DC HMIS will be directed to The Community Partnership. No individual client data will be provided to meet these requests without proper authorization or consent as stated in TCP's Privacy Policy.

Procedure: All requests for data from anyone other than an Authorized Agency or a client will be directed to TCP's Executive Director or her designee. As part of the mission to end homelessness in the District of Columbia, it is The Community Partnership's policy to provide aggregate data on homelessness and housing issues in this area. TCP will also issue periodic public reports about homelessness and housing issues in the District of Columbia. No individually identifiable client data will be reported in any of these documents.

D.13. Data Retrieval Support

Policy: Authorized Agencies will create and run agency-level reports.

Explanation: The Agency Administrator has the ability to create and execute reports on agency-wide data. This allows Authorized Agencies to customize reports and use them to support agency-level goals. The DC HMIS is to be a tool for the Authorized Agencies in managing programs and services.

Procedure: The Agency Administrator will be trained in the use of reporting tools by TCP. The DC HMIS System Administrator will provide query and templates for reports specifically required by TCP, and may assist Agency Administrators with the development of reports/queries for their specific use.

E. Other HMIS Information

E.1. DC HMIS Security Infrastructure

The following information about how DC HMIS data is protected from unauthorized access or use is provided here for the benefit of all Authorized Agencies, public officials, advocates and consumers who are interested in the architecture of security.

Server Hosting at Bowman's Location: TCP has co-located the DC HMIS database and web application servers in Shreveport, Louisiana, at the headquarters of Bowman Internet Services. This is done to take advantage of Bowman's ability to provide 24-hour security and support for TCP's hardware and software. Co-location means that while TCP owns the hardware and software, it pays a monthly maintenance fee for Bowman to provide both server hosting and routine server maintenance.

Bowman employs a full time staff of experts dedicated to keeping their clients up and running, secure, and using the latest technology. This technology includes physical security, Cisco firewalls, authentication through *Verisign* certificates, Windows' secure server technology, and 128-bit encryption of usernames, passwords, and all data passing to and from the database.

It is the job of the DC HMIS System Administrator and TCP's Chief of Policy and Programs to maintain a point of contact between Bowman and TCP and keep track of any security issues related to the hosting of the DC HMIS database.

Physical Attack: The database server and web server are located in a physically secure building where security guards are employed to monitor security from 7:00 a.m. to 7:00 p.m. Monday through Friday, and from 8:00 a.m. to 4:00 p.m. on Saturdays. During off-hours, a card key is required to enter the building. Within the building, the Bowman offices are also locked with a separate key structure. The server itself deploys the standard security measures available in Windows NT 4.0 to prevent unauthorized local access.

Network Attack: Bowman uses Cisco firewalls to prevent unauthorized remote access to the database server. A firewall is a software application that blocks all incoming electronic traffic except traffic that is explicitly permitted. Permissions are configured manually by network administrators. This combination of firewalls and virus protection software will detect and prevent most viruses, trojan horses, worms, malicious mobile codes or email bombs from damaging our database.

Denial of Service: The combination of firewalls and routine monitoring of network traffic by skilled professionals (Bowman network administrators) will detect and prevent an attacker from flooding our server to the point of failure.

Exploitation of Operating System Vulnerabilities: As part of the maintenance contract, network administrators at Bowman are responsible for updating the server with the latest software patches and fixes of known operating system weaknesses. Keeping abreast of software patches and reports of new vulnerabilities is the best way to avoid falling prey to these attacks.

Exploitation of Software Vulnerabilities: Because TCP relies on the same company who created the *ServicePoint* software to host its server, TCP is assured that security holes discovered in the *ServicePoint* software will be addressed by technicians with access to timely and accurate information about the core program. TCP does not need to rely on second or third-hand software alerts or the installation of patches and upgrades by network administrators unfamiliar with the product. This is a great advantage in combating application-specific security issues.

User Falsification: Using a public-key infrastructure and signed digital certificates, the latest security technology available, Verisign provides a safe and reliable method of

authenticating users. These methods, while they do employ traditional user names and passwords at their base, also encrypt data and provide a software-enabled check and counter-check methodology that make stealing identities or masquerading as an authorized user virtually impossible. In addition, these methods produce one-time use session keys that foil a replay attack, as user credentials will never be signed and encrypted in precisely the same way twice.

Data Traps: Verisign provides 128-bit SSL encryption of all data passing from agency to server, or server to agency. Encryption is the translation of data from a readable "clear text" to an encoded hash using complex mathematical algorithms. SSL, short for secure sockets layer, is a data transport protocol that encrypts data using a public-key infrastructure. 128-bit SSL encryption is the strongest encryption allowed by the U.S. Department of Commerce; it is estimated that data encrypted with 128-bit encryption would take a trillion-trillion years to crack using today's technology. When data is encrypted, even if packets could be captured or recorded as they travel across the Internet, they could not be decoded and read.

Server Falsification: The public-key infrastructure provided by Verisign provides not only authentication of the agency, but also authentication of the web site, and hence, authentication of the hosting server. Authentication is provided through digital certificates verified by Verisign, and is an integral part of the login process. Mutual authentication prevents a rogue web site from masquerading as our secure web site and drawing sensitive data.

Social Engineering: These are attacks in which a social situation (for example, a customer service call from a third-party company) is manipulated so that an unauthorized user gains access to protected information, such as client data, or user names and passwords. The biggest deterrent to social engineering is clear policies and procedures. It is much harder for users to be manipulated into providing confidential information if they have clear and thoughtful rules to follow when providing such information. TCP provides clear policies and procedures around issues of *ServicePoint* data confidentiality and confidentiality of user names and passwords. These policies and procedures are designed to speed problem resolution and minimize the chance of a user being manipulated into divulging confidential data through confusion or a sincere desire to help someone in need.

Misuse of Privileges: *ServicePoint* provides several levels of user access to the database. Each level has access to a particular subset of information and particular abilities to manipulate information. TCP provides clear "job descriptions" for each level of access, to ensure that each user is assigned an appropriate level of access. TCP provides clear protocol and procedures for handling data needs and requests that fall outside of a particular user's job description. Finally, TCP will provide clear procedures for handling changes in access levels and users, as well as for password recovery and other access issues. These procedures will be designed to clarify and streamline the daily work of legitimate users, and minimize the chance of legitimate users misusing privileges even towards legitimate ends.

Local Physical Attack: Agency computers are necessarily more physically vulnerable than our central server. As no ServicePoint data is stored on the local computer the physical vulnerability of these computers does not constitute a significant threat to client confidentiality regarding this data. However, any user access data, such as a password, that is stored on a computer or in a written file, does constitute a risk to client confidentiality.

The DC HMIS policies and procedures will include provisions for the appropriate handling of client access data. In addition the physical security for the DC HMIS is enhanced with database level encryption through the purchase of Protegrity software. This two key encryption system works like a safety-deposit box. Even if a computer or server are stolen, (one key), the data is still safe and remains unreadable.

The guidelines set forth in this document are subject to change. This is version 5.0. Effective date November 1, 2015.