DISTRICT OF COLUMBIA COC HMIS POLICIES

HOMELESS MANAGEMENT INFORMATION SYSTEM

VERSION 6.1

EFFECTIVE DATE: OCTOBER 1, 2020

TABLE OF CONTENTS

1. INTRODUCTION

The District of Columbia Homeless Management Information System (DC HMIS) is a collaborative project of the DC Continuum of Care (CoC), The Community Partnership for the Prevention of Homelessness (TCP), the District of Columbia, and participating Partner Agencies. The HMIS is an internet-based database that is used by homeless service organizations within the District of Columbia to record and store client-level information to better understand the numbers, characteristics, and needs of homeless persons and those at risk of homelessness. WellSky Corporation administers the central server and provides the HMIS software, ServicePoint. TCP is the Lead Agency administering the system and managing user and agency licensing, training, and compliance. (Note: TCP is hereinafter referred to as simply the "Lead Agency.")

The HMIS enables service providers to measure the effectiveness of their interventions and facilitate longitudinal analysis of service needs and gaps. Information that is gathered from clients via interviews conducted by service providers is aggregated and made available to policy makers, researchers, service providers, and advocates. Data about the extent and nature of homelessness in the District of Columbia are used to inform public policy decisions aimed at addressing and ending homelessness at local, District, and federal levels.

Guidance for the implementation of the District of Columbia's HMIS is provided by the Continuum of Care's Executive Committee and the workgroups of the Interagency Council on Homelessness (ICH). These entities work closely with the Lead Agency to secure funding, set and manage priorities within available funding, collect and incorporate user feedback, and provide appropriate oversight and guidance. Meeting information for these workgroups and committees are available on the ICH website.

This document provides the policy guidelines and standards that govern HMIS operations and security, as executed by the Lead Agency, and also describes the responsibilities of Partner Agencies and users. It was approved by the ICH Executive Committee on _____ and replaces the earlier document: "District of Columbia Homeless Management Information System Policies and Standard Operating Procedures" (November 2015). It will be reviewed annually by the Lead Agency and the ICH Executive Committee.

1.1 CONTACT INFORMATION

DC's Lead Agency Website:	community-partnership.org
HMIS Helpdesk:	hmis@community-partnership.org
Lead Agency Address:	801 Pennsylvania Ave SE Suite 360 Washington DC, 20003

1.2 PARTICIPATING ENTITIES

Regardless of funding source, entities that may use the HMIS include, but are not limited to:

- Coordinated Entry/CAHP Assessors
- Day Shelters and Drop-in Centers for persons who are homeless
- Emergency Shelters serving homeless adults, families, and youth, including Low Barrier Shelters, Temporary Shelters, Short-term Family Housing Programs, and Severe Weather Shelters

- Transitional Housing programs
- Rapid-Rehousing programs
- Supportive Housing programs
- Street and Community Outreach programs to persons who are homeless
- Supportive Service programs serving persons who are homeless

In addition, HMIS participation is a requirement of various funders. On the Federal level, HMIS participation is mandated for service and housing providers that receive funding (either as a direct grantee or as a sub grantee) through the following agencies and funding sources:

Department of Housing and Urban Development (HUD)

- Continuum of Care Program (CoC)
- Emergency Solutions Grant (ESG)
- Housing for Persons with AIDS (HOPWA)

Department of Health and Human Services (HHS)

- Projects for Assistance in the Transition from Homelessness (PATH)
- Runaway and Homeless Youth Program (RHY)

Department of Veterans Affairs

- Supportive Services for Veteran Families (SSVF)

On the local level, the District of Columbia Department of Human Services and TCP require HMIS participation for their grantees under the following grants:

Department of Human Services (DHS)

- Short-term Family Housing (STFH)
- Comprehensive Street Outreach Network (CSON)
- Homeless Prevention Programs (HPP)
- Rapid Rehousing for Individuals Program (RRH-I)
- Family Reunification and Stabilization Program (FRSP)
- Permanent Supportive Housing Program (PSHP)

The Community Partnership (TCP)

- DHS Management Grants
- DHS Sole Source Grants
- TCP Direct Grants

1.3 FEDERAL POLICIES

In addition to the District of Columbia HMIS Policies contained herein, the DC HMIS must also comply with federal HMIS requirements. These requirements are detailed in a suite of HMIS Data Standard resources, an overview of which is provided below:

Manual Name & Link	Intended Audience	Contents
HMIS Data Standards Dictionary	HMIS Vendors and HMIS Lead Agencies	The manual provides the detailed information required for system programming on all HMIS elements and responses required to be included in HMIS software. It delineates data collection requirements, system logic, and contains the XML and CSV tables and numbers. The manual also includes critical information about data collection stages, federal partner data collection required elements, and metadata data elements.
HMIS Data Standards Manual	HMIS Lead Agencies and HMIS Users	The manual provides a review of all of the Universal Data Elements and Program Descriptor Data Elements. It contains information on data collection requirements, instructions for data collection, and descriptions that the HMIS User will find as a reference.

The documents are typically reviewed and updated each year, and changes tend to be effective October 1, in line with the Federal Fiscal Year.

HMIS Federal Partner Program Manuals contain additional detailed information on HMIS project setup and data collection for federally-funded programs:

- CoC Program Manual
- ESG Program Manual
- HOPWA Program Manual
- PATH Program Manual
- RHY Program Manual
- HUD VASH Program Manual
- VA Program Manual

2. JOINING THE HMIS

While HMIS participation is open to homeless service organizations regardless of funding sources, all Partner Agencies and users must agree to and abide by HMIS policies and procedures and all related requirements. These requirements are described throughout this document, whereas this section focuses specifically on the process of new agencies, projects, and users joining the HMIS.

2.1 PARTNER AGENCY REQUIREMENTS

AGENCY-LEVEL DOCUMENTS

In order to obtain and maintain access to the HMIS, Partner Agencies must complete and adhere to the following documents:

1. **Agency Agreements** define the legal relationship between a Partner Agency and the Lead Agency as it relates to HMIS responsibilities and compliance with policies and procedures. The Agency Agreement must be signed by the Partner Agency's executive director. The Lead Agency will retain the original copy.
2. **Business Associate Agreements** are required for Partner Agencies covered under HIPAA and protect personal health information in accordance with HIPAA guidelines.
3. **Qualified Service Organization Agreements** are required for Partner Agencies covered under Federal Drug and Alcohol Confidentiality Regulations (42 CFR Part 2).

MINIMUM TECHNOLOGY REQUIREMENTS

For proper access to the HMIS, Partner Agencies should meet the following minimum technology requirements:

MINIMUM COMPUTER REQUIREMENTS

- A PC with a 2 Gigahertz or higher processor, 40GB hard drive, 512 MB RAM, and Microsoft Windows 7 (or later)
- The most recent version of Google Chrome, Safari, Internet Explorer, or Firefox. No additional plugin is required. It is recommended that our browser have a 128 cipher/encryption strength installed. The browser's cache should be set to "Check for new version of the stored pages: Every visit to page."
- A broadband internet connection or LAN connection. Dial-up modem connections are not sufficient.
- Virus protection updates
- Mobile devices used for HMIS data entry must use the Mozilla Firefox, Google Chrome, or Apple Safari internet browsers. Apple Safari must be used on the latest version of iOS.

ADDITIONAL RECOMMENDATIONS

- Windows 7: 4Gig memory recommended (2 Gig minimum)
- A Dual Core processor is recommended

Slow system response times that may arise as a result of slow internet connections cannot be controlled by the HMIS Lead Agency.

If your agency is having difficulty obtaining the necessary technology or meeting the minimum computer requirements, please contact the Lead Agency.

STAFF ELIGIBLE TO BECOME HMIS USERS

The Partner Agency must have at least one staff member who is eligible to become an HMIS user. Users must be paid staff of a Partner Agency. Individuals who are solely contracting with a Partner Agency must be subject to the same vetting and training as staff and volunteers who become HMIS users. All users must be at least 18 years old and possess basic computer skills. The Partner Agency is responsible for the actions of its users and for their training and supervision, in accordance with the Agency Agreement.

AGENCY ADMINISTRATOR

The Partner Agency's Executive Director or their designee must select at least one person to act as the Agency Administrator. Multiple Agency Administrators are most appropriate for large agencies that have multiple departments.

DUTIES OF THE AGENCY ADMINISTRATOR

- Serve as the primary contact between the Partner Agency and the Lead Agency
- Provide updated agency information in a timely manner to the Lead Agency for update in the HMIS. This includes providing notification about new projects, new users, closed projects, and users that no longer work at the agency.
- Ensure the quality and accuracy of data entered by agency users.[1]
- Ensure the stability of the agency's connection to the internet and ServicePoint, either directly or in communication with other technical professionals.
- Coordinate the training of all agency end users either as a designated Trainer or by ensuring correct registration and completion of training from the Lead Agency.
- Coordinate the agency's management of Releases of Information (ROIs) received from clients, giving permission to have their information shared with other agencies within HMIS. The Agency Administrator or a designee must upload the ROI to the client's HMIS record.
- Provide support for the generation of agency reports.
- Respond to and coordinate the agency's efforts around the Data Quality policy of HMIS.
- Understand and comply with funder data collection and reporting requirements.
- Monitor and enforce compliance with standards of client confidentiality and ethical data collection, entry, and retrieval at the agency level. This includes security of client data within and extracted from the DC HMIS.
- Respond to Lead Agency's questions, requests for information, etc.

CORE COMPETENCIES OF AGENCY ADMINISTRATORS

- Must be an existing HMIS user, with a valid agency email address, and have completed the HMIS Agency Administrator Training.
- Must be technically proficient with a web-based HMIS as they will be responsible for maintaining the Partner Agency's portion of HMIS.
- Must be in good standing with the Lead Agency and HMIS in terms of User Conduct and training.
    - Must not have any security or policy violations to their name.

[1] In general, domestic violence programs are prohibited from participation in the HMIS by federal legislation, under the Violence Against Women Act (VAWA). Please contact the Lead Agency for additional information.

USE OF A COMPARABLE DATABASE BY VICTIM SERVICE PROVIDERS[1]

Victim service providers, as defined at 24 CFR 576.3, are agencies whose primary mission is to provide services to victims of domestic violence, dating violence, sexual assault, or stalking and are funded with Violence Against Women Act (VAWA) money. Victim service providers must not directly enter or provide data for entry into the HMIS if they are legally prohibited from participating in the HMIS. Individual projects that meet the definition of victim service providers are subject to the same restriction, even if they are a part of an agency whose primary mission is not to provide services to victims of domestic violence, dating violence, sexual assault, or stalking.

Victim service providers that are recipients of funds requiring participation in the HMIS, but are prohibited from entering data in the HMIS, must use a comparable database to enter their client information. A comparable database is a database that can be used to collect client-level data over time and generate unduplicated aggregated reports based on the client information entered. The reports generated by a comparable database must be accurate and provide the same information as the reports generated by the HMIS.

Persons fleeing domestic violence, dating violence, sexual assault, or stalking who are served by non-victim service providers are not prohibited from having their data entered into the HMIS. However, a client may refuse to answer HMIS questions in accordance with the Baseline Privacy Policy outlined in Section 5.1 of these policies. Data sharing is permitted if the client agrees to release their information by signing a Release of Information (ROI).

2.2 NEW PROJECTS

An **HMIS New Provider Setup Form** is required for new Partner Agencies and existing Partner Agencies with new projects. The form, which gathers information such as project funding source, target population(s), and beds, allows the Lead Agency to configure data collection and visibility settings appropriately for the agency in the database. Forms should be submitted at least 10 business days prior to the start of the project to allow enough time for processing. HMIS New Provider Setup Form is available on the Lead Agency's website under https://community-partnership.org/new-agency-and-new-provider-resources/ .

2.3 USER AGREEMENT

In addition to completing New User Training as described in the following section, all users must sign an HMIS User Agreement before being allowed access to the DC HMIS.

An **HMIS User Agreement** listing user policies and responsibilities and stating that the user has completed HMIS training must be signed by each authorized user. An electronic copy must be sent to the Lead Agency before the user is given access to the HMIS. An electronic or hard copy of the original document must be kept by the Partner Agency.

The HMIS User Agreement is only valid during the period a user is employed by or volunteering with the Partner Agency. If a user leaves the Agency and returns or moves to another Partner Agency, a new HMIS User Agreement must be signed before HMIS access is granted. If a user is employed by more than one Partner Agency, an HMIS User Agreement is required for each agency.

USER CONFLICT OF INTEREST

Users who are also clients with files in the DC HMIS are prohibited from entering or editing information in their own file. All users are also prohibited from entering or editing information in files of immediate family members. All users must report any potential conflict of interest to their Agency Administrator. The Lead Agency may run an

HMIS user audit trail report to determine if there has been a violation or suspected violation of this conflict of interest.

3. USER TRAINING REQUIREMENTS

3.1 NEW USER TRAINING

All users are required to attend an HMIS Training approved by the Lead Agency - either provided directly by the Lead Agency or a training administered by the Agency Administrator and approved by the Lead Agency - prior to receiving access to the system.

TIMELY LOGIN

Once a user has completed HMIS Training, they must submit their signed User Agreement and log into HMIS within 60 days of training completion. Failure to do so will result in a user needing to complete HMIS training, or a test of the data entry trained upon in the HMIS Training, and resubmission of their User Agreement before gaining access to the DC HMIS.

SUCCESSFUL COMPLETION

Lead Agency Staff may determine that a new user has failed to grasp the necessary data entry concepts during training. Lead Agency staff may use their discretion to require new users to repeat HMIS Training. If a new user fails to successfully complete HMIS Training after repeated attempts, Lead Agency staff may use their discretion to determine that the new user is not capable of accurate and complete data entry and may refuse to issue the new user a DC HMIS user license. The Lead Agency will work with the user's Agency Administrator to determine next steps needed for the user to be able to gain access to the system, including but not limited to computer training.

EXCEPTIONS

If a user requesting a new user license had a license for the DC HMIS in the past 365 days, the user will be given the option to test out of HMIS Training through a demonstration of fundamental data entry knowledge. The Lead Agency has sole discretion to determine whether the user has successfully tested out of this requirement.

3.2 ONGOING TRAINING

REGULAR LOGIN

Lead Agency Staff monitors the system for regular logins. If a user does not log into the DC HMIS in a six (6) month period of time, Lead Agency Staff will remove the user's access. The user will then need to complete HMIS training, or a test of the data entry trained upon in the HMIS Training before gaining access to the DC HMIS.

ANNUAL SECURITY TRAINING

All users are required to attend annual security training provided by the Lead Agency to retain their user license.

RECERTIFICATION TRAINING

At the discretion of the Lead Agency, users may be required to complete a recertification training for a variety of reasons, e.g., in the event of significant changes to data collection requirements, data entry workflow, or HMIS policies and procedures. Users who do not complete recertification training in a timely fashion may have their licenses suspended until training has been completed.

HMIS TRAINING AS REMEDIAL TRAINING

If the Lead Agency or Agency Administrator determines that data entered by a current user does not meet minimum data quality standards, that user may be denied access and required to repeat the training.

3.3 COORDINATED ACCESS AND HOUSING PLACEMENT (CAHP) TRAINING

VI-SPDAT TRAININGS

All users who are approved to complete VI-SPDATs are required to attend an HMIS VI-SPDAT Training prior to receiving access to the VI-SPDAT portion of the system. These Trainings are open to existing HMIS users and approved CAHP participating agencies.

REMEDIAL TRAINING

If the Lead Agency or Agency Administrator determines that data entered by a current user does not meet minimum data quality standards, that user may be required to repeat the training.

FULL SPDAT AND FAMILY SPDAT TRAININGS

In order to gain access to the full SPDAT measurement section of the system, a user must complete the VI-SPDAT training and the full training for the SPDAT relevant to their subpopulation (families, youth or individuals) provided by the Lead Agency. These Trainings are open to existing HMIS users and approved CAHP participating agencies.

3.4 AGENCY ADMINISTRATOR TRAINING

In order to become an Agency Administrator, a user must have successfully completed HMIS Training for the various program types their Agency has and then must successfully complete the Agency Administrator Training. The Agency Administrator Training covers proper communication channels with the Lead Agency as well as system duties for Agency Administrators.

The Lead Agency may require that an Agency Administrator complete the Agency Administrator Training if the Lead Agency feels the Agency Administrator is not grasping the necessary pieces of information to successfully fulfill the role of Agency Administrator.

4. DATA SECURITY

The Lead Agency, Local Contract Monitors, and Partner Agencies are jointly responsible for ensuring that HMIS data processing capabilities, including the collection, maintenance, use, disclosure, transmission, and destruction of data, comply with the HMIS security policies and procedures. When a security standard conflicts with other federal, district, and local laws to which the Partner Agency must adhere, the Partner Agency must contact the Lead Agency to collaboratively update the applicable policies for the Partner Agency to accurately reflect the additional protections.

4.1 USER ACCESS

Agency Administrators will provide unique user names and initial temporary passwords to each Partner Agency user. User names will not be exchanged or shared with other users. The Lead Agency will have access to the track user name distribution and user.

4.2 PASSWORDS

Passwords are the individual's responsibility and users cannot share passwords. Any passwords that are written down are to be stored securely and must be inaccessible to other persons. Users are not to store passwords on a personal computer for easier log on.

4.3 PROCEDURE FOR REPORTING SECURITY INCIDENTS

Users and Agency Administrators should report all unlawful access of the HMIS and unlawful attempted access of the HMIS. This includes borrowing, loaning, sharing, or theft of user names and passwords. Security incidents should be reported to the Lead Agency within 24 hours of their discovery. The Lead Agency will use the HMIS user audit trail report to determine the extent of the breach of security.

4.4 VIOLATION OF SECURITY PROCEDURES

All potential violations of any security protocols will be investigated by the Lead Agency and any user found to be in violation of security protocols will be sanctioned accordingly. Sanctions may include but are not limited to: a written notice of the violation, suspension of system privileges, revocation of system privileges, and referral for criminal prosecution.

All confirmed security violations will be communicated in writing to the affected client within 14 days, unless the client cannot be located. If the client cannot be located, a written description of the violation and efforts to locate the client will be prepared by the Lead Agency and placed in the client's file at the Agency that originated the client's record.

Any Agency that is found to have consistently and/or flagrantly violated security procedures may have their access privileges suspended or revoked, as described in Section 9.

4.5 DISASTER RECOVERY PLAN

DC HMIS is covered under the WellSky Community Services Disaster Recovery Plan. Due to the nature of technology, unforeseen service outages may occur. In order to assure service reliability, WellSky provides the following disaster recovery plan. Plan highlights include:

- Database tape backups occur nightly.
- Tape backups are stored offsite.
- Seven-day backup history is stored locally on instantly accessible Raid 10 storage.
- One-month back up history is stored offsite.
- Access to a WellSky emergency line to provide assistance related to “outages” or “downtime” 24 hours a day.
- Data is backed up locally on instantly accessible disk storage every 24 hours.
- The application service is backed up offsite, out-of-state, on a different internet provider and on a separate electrical grid via secured Virtual Private Network (VPN) connection.
- Backups of the application site are near-instantaneous (no files older than five minutes).
- The database is replicated nightly at an offsite location in case of a primary data center failure.
- Priority-level response (ensures downtime will not exceed four hours).

5. DATA PRIVACY

The Lead Agency, Local Contract Monitors, and Partner Agencies are jointly responsible for complying with HMIS privacy policies and procedures. When a privacy standard conflicts with other federal, district, and local laws to which the Partner Agency must adhere, the Partner Agency must contact the Lead Agency to collaboratively update the applicable policies for the Partner Agency to accurately reflect the additional protections.

5.1 BASELINE PRIVACY POLICY

COLLECTION OF PERSONAL INFORMATION

Personal information will be collected for the HMIS only when it is needed to provide services, when it is needed for another specific purpose of the agency where a client is receiving services, or when it is required by law. Personal information may be collected for these purposes:

- To provide or coordinate services for clients
- To find programs that may provide additional client assistance
- To comply with government and grant reporting obligations
- To assess the state of homelessness in the community, and to assess the condition and availability of affordable housing to better target services and resources

Personal information may also be collected from:

- Additional individuals seeking services with a client
- Other private organizations that provide services and participate in the HMIS

Only lawful and fair means are used to collect personal information. Personal information shall be collected with the knowledge and consent of clients. While some information may be required by projects or public or private funders to determine eligibility for housing or services, or to assess needed services, clients generally should not be denied assistance if they refuse or are unable to supply certain pieces of information.

POSTED HMIS DATA PRIVACY NOTICE

The Notice must be posted and viewable by clients at intake to provide information on their rights and HMIS policies related to personal data. This Notice provides a brief overview of data privacy. While Partner Agencies may use their own Privacy Notice, it must include at minimum the information included on the standard District of Columbia Posted HMIS Data Privacy Notice as seen in Appendix B.

HMIS DATA PRIVACY NOTICE

This Notice must be reviewed with all clients at intake to provide information on their rights and HMIS policies related to personal data. This Notice provides more detailed information about why HMIS data is collected, when and to whom data may be released, privacy protections, and client rights.

INSPECTION AND CORRECTION OF PERSONAL INFORMATION

Clients may inspect and receive a copy of their personal information maintained in the HMIS as well as a logged audit trail of changes to those records. The agency where the client receives services will offer to explain any information that a client may not understand.

If the information listed in the HMIS is believed to be inaccurate or incomplete, a client may submit a verbal or written request to have their information corrected. Inaccurate or incomplete data may be deleted or marked as inaccurate or incomplete and supplemented with additional information.

A request to inspect of copy one's personal information may be denied if:

- The information was compiled in reasonable anticipation of litigation or comparable proceedings, or is subject to a legally recognized privilege, e.g., attorney-client,
- The information was obtained under a promise of confidentiality and if the disclosure would reveal the source of the information, or
- The life of physical safety of any individual would be reasonably endangered by disclosure of the personal information.

If a client's request to view or correct their personal information is denied, the Agency where the client receives services will explain the reason for the denial. The client's request and the reason for the denial will be included in the client's record. As noted below in 5.4, Client is entitled to challenge an Agency's denial. Partner Agency is responsible for advising Client of their right to appeal a denial to review or change information,

Client requests to view or correct their personal information may be denied if they are made in a repeated and/or harassing manner.

5.2 DATA SHARING

The sharing of data between Partner Agencies within the DC HMIS is currently limited to client demographics. This sharing is for the purpose of reducing the duplication of client records within the DC HMIS, to minimize repetitious questioning of clients, and to ensure a stronger Coordinated Entry System process.

The following pieces of client information are shared between all Partner Agencies within the DC HMIS:

- Client Name
- Client Name Data Quality
- Client Social Security Number
- Client Social Security Number Data Quality
- Client Date of Birth
- Client Date of Birth Data Quality
- Client Race
- Client Ethnicity
- Client Gender
- Client Veteran Status

All other client information is not shared between Partner Agencies unless a Release of Information is signed.

CLIENT RELEASE OF INFORMATION

The sharing of client program data between Partner Agencies within the DC HMIS is a process that is guided by the client through the Release of Information (ROI). It is therefore imperative that the client understands the ROI, and that the Partner Agency address any questions the client may have, while respecting the client's right to decline to share data.

Prior to designating any information for sharing with other Agencies, the Partner Agency will obtain the informed consent of the client, using a Release of Information. If a client does not consent via a Release of Information, information may be entered into the DC HMIS but may not be shared with other Partner Agencies. It is the responsibility of the Partner Agency entering information about a client to determine whether consent has been obtained; to make appropriate entries to either designate the information as appropriate for sharing or prohibit information sharing; and to implement any restrictions on information sharing.

AGENCY RESPONSIBILITIES

When an Agency uses a Release of Information to allow for sharing between Agencies within the DC HMIS the Partner Agency must, at a minimum, meet the following standards:

1. The Partner Agency will use a Release of Information that has been approved by the Lead Agency for the use with the DC HMIS for all clients where written or verbal consent is required.
2. The Partner Agency will note any limitations or restrictions on information sharing on a client's ROI with appropriate data entries into the DC HMIS.
3. The Partner Agency will be responsible for ensuring that consent is knowing, informed, and given by a person competent to provide consent.
4. If a client withdraws or revokes consent for release of information, the Partner Agency is responsible for immediately contacting the Lead Agency to ensure that the client's information will not be shared with other Agencies from that date forward.
5. The Partner Agency that received the client's release of information will scan and upload the signed copy of the form to the DC HMIS. Partner Agencies may be required to keep the original copy for a period of seven (7) years, as dictated by Partner Agency policy or funder requirements. ROI forms will be available for inspection and copying by the Lead Agency at any time.

ADDITIONAL RESPONSIBILITIES OF COVERED ENTITIES

Partner Agencies that are also Covered Entities under HIPAA and any program subject to 42 CFR Part 2 must ensure that their Release of Information has the proper coverage for the additional data privacy requirements. A Release of Information is required to be signed before authorizing the Lead Agency to use or disclose information entered into the DC HMIS by a Covered Entity. If a client does not sign a Release of Information for a Covered Entity information may be entered into the DC HMIS but may not be further disclosed. The information may be used by the Lead Agency as permitted by law and the HMIS Data Privacy Notice.

It is the responsibility of the Partner Agency entering information about a client to ensure compliance with HIPAA including ensuring that all appropriate HIPAA Notices have been provided to clients, to determine whether consent has been obtained; making appropriate entries to either designate the information appropriate for use or disclosure by the Lead Agency or to prohibit such use or disclosure; and implementing any restrictions on the use of the information.

NO CONDITIONING OF SERVICES

The Partner Agency will not condition any services upon or decline to provide any services to a client based upon a client's refusal to sign a form for the sharing of information in the DC HMIS, unless a program funder requires the entry of identified information into the HMIS to deliver services. Further, Partner Agencies may not limit client service or refuse to provide services in a way that discriminates against clients based on information the Partner Agency obtained from the DC HMIS or for any other reasons prohibited by law. Partner Agencies may not penalize a client based on historical data contained in the DC HMIS.

5.3 RESEARCH USES AND PUBLICATION OF HMIS DATA

Research uses and publication of HMIS data are governed by HMIS policies, including the HMIS Data Privacy Notice, Agency Agreements, and Business Associate Agreements.

Data may not be released in an aggregated report from a data set that is either small or unique enough to allow identification of an individual client's information to be extracted from the report. If it is determined that a preliminary report may not be published due to concerns of release of identifiable data, the Lead Agency will remove postings, shred paper copies of the report, and notify review partners to destroy any copies of the report.

If a report identifies one or more specific agencies or programs, agencies will be given a period of 15 business days to review and comment in the information as presented in the report. Agency Review periods may be waived if prior approval is obtained by the Lead Agency.

Data may be released to external stakeholders for research purposes by the Lead Agency. The Lead Agency will approve or deny requests to release data based on the potential benefits and costs to client, Partner Agencies, and other stakeholders. If at all possible, the release of identified data will be avoided. If identifiable data is needed, the Lead Agency to ensure that proper procedures and precautions are in place prior to releasing data.

5.4 CLIENT COMPLAINTS, GRIEVANCES, AND QUESTIONS

If a client believes that their rights have been violated related to their personal or private data held in the DC HMIS, a written complaint may be filed. The complaint may be filed with the Partner Agency serving the client and forwarded to the Lead Agency if resolution is not found. If the client believes that their shelter or services may be threatened due to the complaint, a complaint may be made directly to the Lead Agency. The Lead Agency will report all grievances to the Executive Committee, which will act as a final arbiter of any complaints not resolved by the Partner Agency or the Lead Agency.

The Partner Agency and the Lead Agency are prohibited from retaliating against clients for filing a complaint. Identifying information will be kept confidential, unless the client gives express permission for such information to be shared between the Partner Agency and the Lead Agency.

The Partner Agency must make the DC HMIS Service Recipient Grievance Form (Appendix C) available to clients upon request.

6. DATA QUALITY

Data Quality is a term that refers to the reliability and validity of client-level data collected in the DC HMIS. It is measured by the extent to which the client data in the system reflects actual information in the real world. No data collection system has a quality rating of 100%. However, to present accurate and consistent information on homelessness, it is critical that the DC HMIS have the best possible representation of reality as it relates to persons experiencing homelessness and the projects that serve them. Specifically, the goal is to record the most accurate, consistent, and timely information in order to draw reasonable conclusions about the extent of homelessness and the impact on the homeless service system in the District of Columbia.

6.1 MINIMUM DATA COLLECTION STANDARDS

All Partner Agencies are responsible for asking all clients a minimum set of questions, or data elements. These required data elements include:

1. The Universal Data Elements required federally and at the District level by the CoC Executive Committee
2. Program-Specific Data elements, which depend on the funder and may not be required at all if a program is not funded by a grant that requires the use of the HMIS.

The minimum expectations for data entry for all programs entering data in the HMIS are the focus of the HMIS User Training.

Partner Agency programs are configured by the Lead Agency to collect the required data elements based on information provided by the Partner Agency and its Agency Administrator. Lead Agency staff will consult with the Agency Administrator in attempts to ensure proper set up, but responsibility for complying with funder requirements lies with the Partner Agency.

Agencies may collect additional information beyond the minimum required data elements, as long as the collection of these questions does not interfere with the minimum required data elements.

6.2 DATA QUALITY PLAN

To ensure high-quality data, the Lead Agency, Partner Agencies, and users will regularly and collectively assess and address the quality of data by examining characteristics such as timeliness, completeness, and accuracy. This effort is detailed in the DC HMIS Data Quality Plan.

7. HMIS SOFTWARE VENDOR REQUIREMENTS

PHYSICAL SECURITY

Access to areas containing HMIS equipment, data and software will be secured.

FIREWALL PROTECTION

The vendor will secure the perimeter of its network using technology from firewall vendors. Company system administrators monitor firewall logs to determine unusual patterns and possible system vulnerabilities.

USER AUTHENTICATION

Users may only access the DC HMIS with a valid user name and password combination that is encrypted via SSL for internet transmission to prevent theft. If a user enters an invalid password three consecutive times, they are automatically shut out of that HMIS session. For added security, the session key is automatically scrambled and re-established in the background at regular intervals.

APPLICATION SECURITY

HMIS users will be assigned a system access level that restricts their access to only necessary and appropriate data.

DATABASE SECURITY

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

TECHNICAL SUPPORT

The vendor will assist the Lead Agency staff to resolve software problems, make necessary modifications for special programming, and will explain system functionality to the Lead Agency.

TECHNICAL PERFORMANCE

The vendor maintains the system, including data backup, data retrieval, and server functionality/operation. Upgrades to the system software will be continuously developed and implemented.

HARDWARE DISPOSAL

Data stored on broken equipment or equipment intended for disposal will be destroyed using industry standard procedures.

8. FUNDING MONITORS

The DC HMIS is a collaborative partnership with partners at all levels working to advance HMIS as a tool to inform and support efforts to end homelessness. Funding Monitors are key partners in analyzing data and meeting needs at a local level. While Funding Monitors must adhere to all policies contained in this document, this section enumerates roles, responsibilities, and policies specific to their work.

8.1 COORDINATION WITH THE LEAD AGENCY

As the capacity and needs of each Funding Monitor may vary, Funding Monitors will coordinate with the Lead Agency on the roles and responsibilities delegated to the Funding Monitor. The Lead Agency will determine, based on this coordination, the most appropriate user level for each Funding Monitor.

General responsibilities of the Funding Monitor include:

- Ensuring the funding grantees are meeting minimum requirements for clients served
    - Conducting Audits
    - Running counts reports for their grants
- Supporting Lead Agency efforts around:
    - Quarterly Data Quality Process
    - Longitudinal System Analysis
    - Housing Inventory Count
    - Point-in-Time Count
    - System Performance Measures
    - Maintaining and increasing bed coverage (participation of homeless programs in the HMIS)
    - Weekly Occupancy Report
- Other projects or tasks as jointly approved by the parties

8.2 SYSTEM CONFIGURATION

Funding Monitors will not make changes to the HMIS system structure nor any HMIS providers. However, Funding Monitors are allowed to create their own reporting groups in the HMIS for the purposes of aggregate reporting.

8.3 DATA ENTRY

Funding Monitors are prohibited from completing data entry for any program or provider that they monitor. Data entry as a funding monitor is limited to notes on a client file or file attachments and must be stated as coming from a Funding Monitor.

Funding Monitors will direct all data entry and HMIS questions to the HMIS Helpdesk. Funding Monitors will not change HMIS data entry workflows without coordination and approval by the Lead Agency prior to any changes. Training of End Users on all HMIS workflows will remain the responsibility of the Lead Agency.

8.4 FUNDING MONITOR EXPANDED REPORTING ACCESS AGREEMENT

The Lead Agency has developed the Funding Monitor Expanded Reporting Access Agreement to address concerns around limited data visibility in reporting. This agreement, between the Lead Agency and the Funding Monitor, technically grants full visibility to all data in the DC HMIS in the Advanced Reporting Tool (ART) which is used to

report on HMIS data. However, the agreement reaffirms that the Funding Monitor may only view data that is used/created by their grantees as needed for legitimate business purposes.

9. VIOLATIONS OF HMIS POLICIES

HMIS users and Partner Agencies must abide by all HMIS policies and procedures found in the HMIS Policies and/Procedures manuals, the User Agreement, and the Agency Agreement. Repercussions for any violation will be assessed in a tiered manner. Each user or Partner Agency violation will face successive consequences – the violations do not need to be of the same type in order to be considered second or third violations. User violations do not expire. No regard is given to the duration of time that occurs between successive violations of the HMIS policies and procedures as it relates to corrective action.

- **First Violation –** the user and Partner Agency will be notified of the violation in writing by the Lead Agency. The user's license will be suspended for 30 days, or until the Partner Agency notifies the Lead Agency of action taken to remedy the violation. The Lead Agency will provide necessary training to the user and/or the Partner Agency to ensure the violation does not continue.
- **Second Violation –** The user and Partner Agency will be notified of the violation in writing by the Lead Agency. The user's license will be suspended for 30 days. The user and/or the Partner Agency must take action to remedy the violation; however, this action will not shorten the length of the license suspension. If the violation has not been remedied by the end of the 30-day user license suspension, the suspension will continue until the Partner Agency notifies the Lead Agency of the action taken to remedy the violation. The Lead Agency will provide necessary training to the user and/or the Partner Agency to ensure the violation does not continue.

- **Third Violation –** the user and Partner Agency will be notified of the violation in writing by the Lead Agency. The Lead Agency will convene a review panel made up of Lead Agency Staff who will determine if the user's license should be terminated. The user's license will be suspended for a minimum of 30 days, or until Lead Agency review panel makes their determination, whichever occurs later. If the Lead Agency review panel determines the user should retain their user license, the Lead Agency will provide necessary training to the user and/or Partner Agency to ensure the violation does not continue. If users who retain their license after their third violation have an additional violation, that violation will be reviewed by the Lead Agency review panel.

NOTIFYING THE HMIS LEAD AGENCY OF A VIOLATION

It is the responsibility of each Agency Administrator and user to notify the HMIS Lead Agency within 24 hours when they suspect that a User or Partner Agency has violated any HMIS operational agreement, policy, security protocol, or procedure. A complaint about a potential violation must include the User and Partner Agency name a description of the violation, including the date or timeframe of the suspected violation. Complaints should be sent in writing to the HMIS Lead Agency at HMIS@community-partnership.org. The name of the person making the complaint will not be released from the HMIS Lead Agency if the individual wishes to remain anonymous.

VIOLATIONS OF LOCAL, DISTRICT, OR FEDERAL LAW

Any Partner Agency or user violation of local, district, or federal law will immediately be subject to the consequences listed under the Third Violation above.

POTENTIAL TO ESCALATE

All violations will be assessed by the Lead Agency and depending on their severity may be subject to the consequences listed under the Third Violation above as determined by the Lead Agency.

MULTIPLE VIOLATIONS WITHIN A 12-MONTH TIMEFRAME

During a 12-month calendar year, if there are multiple users (three or more) with multiple violations (2 or more) from one Partner Agency, the Partner Agency as a whole will be subject to the consequences listed under the Third Violation above.

10. APPENDICES

APPENDIX A: GLOSSARY

Agency Administrator – The person, designated by the Partner Agency's Executive Director, responsible for system administration at the agency level. This person is specifically trained and responsible for maintaining user accounts, providing introductory training to end users, basic troubleshooting support to end users, maintaining data quality and data security for all HMIS participating programs, reporting any issues within the DC HMIS to the Lead Agency, and being the primary contact for the DC HMIS Lead Agency at their agency.

CAHP – Coordinated Assessment and Housing Placement. DC CoC's Coordinated Entry System

Homeless Management Information System (HMIS) – an internet-based database that is used by homeless service organizations across the District of Columbia to record and store client-level information to better understand the numbers, characteristics, and needs of homeless persons and those at risk of homelessness.

HMIS Lead Agency – the Agency responsible for the technical design, implementation, and operation of the HMIS. In doing so, the Lead Agency provides Partner Agencies and users with training and technical support, ensures compliance with HMIS policies and procedures, and plans the work for the HMIS. DC's HMIS Lead Agency is the Community Partnership for the Prevention of Homelessness.

HMIS Vendor – The HMIS Vendor designs the HMIS software and provides ongoing support to the System Administrators. DC's HMIS Vendor is WellSky.

Interagency Council on Homelessness (ICH) - A local partner that serves as the governing board of the DC CoC. They are responsible for the DC Strategic Plan, policy development, strategic partnerships, interagency coordination, and final oversight of the DC HMIS.

Partner Agencies – The homeless service organizations that use the DC HMIS.

Program-Specific Data Elements – Questions that are designed, managed, and required by at least one of the HMIS federal or district partner programs. Federal Program-Specific Data Elements are subject to change every year on October 1st whereas District Program-Specific Data elements do not have a scheduled time for changes at this time.

Universal Data Elements (UDEs) – The minimum set of questions that all homeless programs in the DC HMIS, regardless of funding source, must complete for all clients served. Federal UDEs are outlined in the HMIS Data Dictionary and the HMIS Data Standards Manual and are subject to change every year on October 1.

Victim Service Provider – a nonprofit agency with a primary mission to provide services to victims of domestic violence, dating violence, sexual assault, or stalking.

DISTRICT OF COLUMBIA: DC HMIS POSTED DATA PRIVACY NOTICE

We collect personal information about the people we serve in a computer system called the DC HMIS (Homeless Management Information System). Many social service agencies use this computer system.

We use the personal information to run our programs and to help us improve services. Also, we are required to collect some personal information by organizations that fund our program.

You do not have to give us information. However, without your information we may not be able to help you. Also, we may not be able to get help for you from other agencies.

You have a right to review the personal information that we have about you. If you find mistakes, you can ask us to correct them. You have a right to file a complaint if you feel that your data privacy rights have been violated.

Please tell our staff if you have questions. If you need a grievance form or a complete copy of our privacy policy, please ask our agency staff.

SERVICE RECIPIENT GRIEVANCE FORM: DC'S HMIS

If you believe that your rights have been violated concerning your personal or private data held in DC's HMIS, you may send a written complaint to:

1. The Agency responsible for providing services to you

If you believe your grievance has not been sufficiently resolved by the service provider agency, you may ask that your complaint be forwarded to The Community Partnership (contact information below). If you believe that your shelter or services may be threatened due to filing a complaint, you may submit your complaint directly to The Community Partnership at:

2. The Community Partnership for the Prevention of Homelessness
   801 Pennsylvania Ave SE, STE 360
   Washington, DC 20003
   hmis@community-partnership.org

TCP will attempt a voluntary resolution of the complaint.

The Agency will report all complaints received to TCP. All complaints received by TCP and their resolutions will be reported to TCP's Executive Director, who will also act as final arbiter of any complaints not resolved by the servicing agency or by TCP's HMIS Staff.

This Agency and TCP are prohibited by law (§§ 4-754.11 – 4-754.13) from retaliating against you for filing a complaint. Your information and complaint will be kept confidential. This Agency and TCP are required by law to maintain the privacy of your protected personal information and to provide you with a grievance procedure.

---

1. To be completed by Service Recipient:

Your name: _____

Agency Name: _____ Program/Shelter Name: _____

Your grievance (what happened, when, where):

What outcome would you like?

Signature: _____ Date: _____

If you are submitting this complaint directly to TCP, stop and submit using the contact information above. If you are submitting this complaint to the Agency, continue to step 2 and provide this form to Agency staff.

2. To be completed by Program Staff

Your name: _____ Your position: _____

Date complaint received: _____

Recommended grievance solution:

Date delivered to service recipient: _____ Delivered by (staff name): _____

3. To be completed by Service Recipient

I am _____ I am not _____ satisfied with the recommended solution.

I wish to take this grievance to the next step by forwarding my concern to the HMIS Lead Agency, and give permission to the Agency to share my identifying information with the HMIS Lead Agency. _____

Signature: _____ Date: _____

4. To be completed by Lead Agency:

Staff member name: _____ Position: _____

Date grievance received: _____

Recommended grievance solution:

Date Delivered to Executive Director: _____ Delivered by (staff name): _____