Arlington County CoC
Homeless Management Information System (HMIS) Governance

June 2017

Table of Contents

Contact Information

Arlington County Govt. Dept. of Human Services

2100 Washington Blvd.
Arlington VA, 22204
Phone: 703-228-3500
Fax: 708-236-3299
Web: www.arlingtonva.us

Staff and Support

Tony Turnage

Homeless Program Manager
Phone: 703-228-1319
Email: tturnage@arlingtonva.us

Ahmad Haj Ali

HMIS Lead/Administrator
Phone: 703-228-1371
Email: ahajali@arlingtonva.us

HMIS Links

HMIS/ETO Software: www.etosoftware.com

ETO Support Manuals:
Link includes the following: (HMIS End User Training, HMIS Reporting, Housing Supplement, Management Supplement)
https://sites.google.com/site/etosoftwarehelpmanual/home/organizations/arlington

Arlington County 10 Year Plan to End Homelessness:
https://publicassistance.arlingtonva.us/10yp/

HOMELESSNESS MANAGEMENT INFORMATION SYSTEM
GOVERNANCE

This manual is developed by the HMIS Governance Committee and authorized by the Executive Committee of the 10 Year Plan to End Homelessness in Arlington County

HMIS GOVERNANCE CHARTER

INTRODUCTION

The Arlington County Government is the lead agency and Collaborative Applicant for the Arlington County Continuum of Care (CoC, VA-600) as well as the designated lead agency for the Arlington County Homeless Management Information System (HMIS). The coverage area for both the CoC and the HMIS includes all municipalities in Arlington County Virginia. The County has primary responsibility for all HMIS activities.

The HMIS Governance Charter serves to delineate the roles and responsibilities related to key aspects of the governance and operations of the Arlington County HMIS. The Policy includes privacy, security, client consent and data entry requirements and may be modified from time to time at the CoC's discretion.

The United States Department of Housing and Urban Development (HUD) requires all grantees and sub-grantees to participate in their local Homeless Management Information System. This policy is consistent with the Congressional direction for communities to provide data to HUD on the extent and nature of homelessness and the effectiveness of its service delivery system in preventing and ending homelessness.

The HMIS and its operating policies and procedures are structured to comply with the most recently released *HUD Data and Technical Standards for HMIS*. Recognizing that the Health Insurance Portability and Accountability Act (HIPAA) and other Federal, State and local laws may further regulate agencies (such as agencies whose primary mission is to provide services to victims of domestic violence, dating violence, sexual assault or stalking), the Continuum may negotiate its procedures and/or execute appropriate business agreements with Partner Agencies so they are in compliance with applicable laws.

The CoC uses all submitted data for analytic and administrative purposes, including the preparation of CoC reports to funders and the Continuum's participation in the Federal Annual Homeless Assessment Report (AHAR). Aggregate data taken from the HMIS is used to inform Strategic Planning activities and the Consolidated Plans of Arlington County.

KEY SUPPORT ROLES & RESPONSIBILITIES

Arlington County Government

As lead agency for the Arlington County Continuum of Care (CoC), the Department of Human Services (DHS):

- Serve as the HMIS lead, oversees the HMIS project and has primary responsibility for all HMIS activities
- Ensures HMIS compliance with all HUD rules and regulations
- Encourages and facilitates participation.
- Approves and facilitates enforcement of HMIS policies as set forth in the *HMIS Governance*
- Supports the HMIS committee
- Designates software to be used for the HMIS in the geographic region
- Selects, approves and executes annual contract(s) with HMIS vendor(s)
- Supervises contract(s) with vendor(s)
- Provides training and support to partner agency users
- Facilitates continuing quality improvement via data analyses and knowledge of best practices
- Provides consolidated Program Type Quarterly/Annually CoC Report Card
- Acts as liaison between the CoC and regional or national HMIS related organizations and participates in related activities

HMIS Committee – Data & Evaluation (D&E) Committee

- Guides the management of the Homeless Management Information System
- Develops, informs, and reviews HMIS policies and procedures
- Advises and recommends to the CoC board changes to HMIS policies and procedures
- Cultivates ways in which future data measurement can contribute to fulfillment of strategic goals
- Is appointed by the CoC Executive Committee
- Consists of the HMIS Agency Administrators, the Arlington County DHS Homeless Programs staff and any members of the public
- Makes recommendations regarding end user data quality assurance and compliance

- Monitors data quality in accordance with Data Quality Plan benchmarks as set forth in the *HMIS Governanc*e
- Ensures compliance with HMIS policies and HUD/State requirements

HMIS Partner Agencies

- Execute an HMIS Agency Partner Agreement annually
- Agree to abide by the most current *HMIS Policy and Procedures Manual* (Policy), also referred to as the Standard Operating Procedures (SOP), approved and adopted by the CoC
- Ensure that all end users comply with the Policy
- Ensure staffing and equipment necessary to implement and ensure HMIS participation

HMIS Agency Administrators

- Are the liaisons between the HMIS Lead/Administrator and their respective agency's end users
- Ensure compliance with HMIS policies within their agency
- Provide support for HMIS use within their agencies (Agency Administrators)
- Provide initial end user training to agency staff
- Provide on-site support to the agency's end-users
- Run agency reports, monitor the agency's data quality, and work with the HMIS Lead/Administrator to troubleshoot HMIS issues
- Attend HMIS related meetings

HMIS Agency Staff

- Includes representatives of all HMIS participating agencies
- Provides feedback on system performance and the need for system enhancements
- Provides input and support for policy application
- Provides information link between agency users and the HMIS Agency Administrators

HMIS Agency Implementation Policies and Procedures

HMIS Participation Policy

Mandated Participation

All projects that are authorized under HUD's McKinney-Vento Act as amended by the HEARTH Act to provide homeless services, projects receiving Arlington County Department of Human Services homelessness funding, and Virginia State funded programs must meet the minimum HMIS participation standards as defined by this Governance. These participating agencies will be required to comply with all applicable operating procedures and must agree to execute and comply with an HMIS Agency Partner Agreement.

Minimum Participation Standards

- Each participating agency shall execute an HMIS Agency Partner Agreement
- Agency staff shall collect the universal and program-specific data elements as defined by HUD and other data elements as determined by the HMIS Committee for all clients served by programs participating in HMIS; data may be shared with other agencies subject to appropriate client consent.
- Agency staff is required to enter the following information within two (2) business days: program enrollments, HUD required demographics, and client entry/exit HUD Assessment Touchpoints.
- Participating agencies shall comply with all HUD regulations for HMIS participation.
- Each agency shall designate two HMIS Agency Administrators who will serve as the primary point person.
- Each HMIS participating project within an agency is required to have a representative at each HMIS related meeting who can effectively communicate what is covered in the meeting to the rest of the project's HMIS users.
- Agencies with programs whose primary focus is to provide services to victims of domestic violence, dating violence, sexual assault or stalking are excluded from mandated participation as per the Violence Against Women Act (VAWA).

HMIS Partnership Termination

In the event that the relationship between the CoC HMIS and a Partner Agency is terminated, the Partner Agency will no longer have access to the HMIS. In the event that a Partner Agency discontinues services within Arlington County, the Partner Agency will no longer have access to the HMIS.

HMIS Security Plan

The Continuum has defined a security plan that:

- Ensures the confidentiality, integrity, and availability of all HMIS information
- Protects against any reasonably anticipated threats or hazards to security
- Ensures compliance by end-users
- HIPAA, VAWA, HOPWA and 42CFR compliant
- HMIS Lead/Administrator will conduct annual audits to ensure compliance with the HMIS Security Plan

HARDWARE, CONNECTIVITY AND COMPUTER SECURITY REQUIREMENTS

Workstation Specification

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

- Operating System: Any system capable of running a current Internet browser as specified below
- Web Browser: The most current version of Microsoft Internet Explorer
- Computers must be securely locked when not in use

Internet Connectivity

Partner Agencies must have Internet connectivity for each workstation accessing the HMIS. To optimize performance, all agencies are encouraged to secure a high speed Internet connection with a cable modem, DSL or T1 line. Any network that has a Wi-Fi component must employ at least WPA2 level security. Use of unsecured public Wi-Fi is strictly prohibited.

Security Hardware/Software

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

Agency Workstation Access Control

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

HMIS USER IMPLEMENTATION

Eligible Users

Each Partner Agency shall authorize use of the HMIS only to users who need access to the system for data entry, editing of client records, viewing of client records, report writing, administration or other essential activity associated with carrying out participating agency responsibilities.

The HMIS Lead/Administrator shall authorize use of the HMIS only to users who need access to the system for technical administration of the system, report writing, data analysis and report generation, back-up administration or other essential activity associated with carrying out central server responsibilities.

User Requirements

Prior to being granted a username and password, users must sign an HMIS Agency End-User agreement that acknowledges receipt of a copy of the agency's privacy notice and that pledges to comply with the privacy notice.

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

Volunteers have the same user requirements that paid staff have. They must have an individual user account, go through the same training, and have the same confidentiality and privacy documents signed and on file with the agency they are serving. The Agency Administrator is responsible for ensuring that the user understands and complies with all applicable HMIS policies and procedures.

Agency Administrators must ensure that users have received adequate training prior to being given access to the database.

Setting Up a New User

- Determine the access level of the proposed HMIS end-user
- Execute an HMIS user confidentiality agreement
- Review HMIS records about previous users to ensure that the individual does not have previous violations with the HMIS Policies and Procedures that prohibit their access to the HMIS
- Verify that an HMIS user confidentiality agreement has been correctly executed
- Verify that appropriate and sufficient training has been successfully completed
- Agency Administrators will then create the new user ID and password in ETO, or submit request for creation to the HMIS Lead Administrator if assistance is needed

Disabling/Terminating User

- If any user leaves the agency or no longer needs access to the HMIS, the Agency Administrator is responsible for immediately terminating user access by disabling the user account, and notifying the HMIS Lead/Administrator.

Enforcement Mechanisms

The HMIS Lead/Administrator will investigate all potential violations of any security protocols. Any user found to be in violation of security protocols will be sanctioned.

Sanctions include, but are not limited to:

- A formal letter of reprimand
- Suspension of system privileges
- Revocation of system privileges

A Partner Agency's access may also be suspended or revoked if serious or repeated violation(s) of HMIS Policies and Procedures occur by agency users.

HMIS Agency Implementation

Adding Partner Agencies

Prior to setting up a new Partner Agency within the HMIS database, the HMIS Lead/Administrator shall:

- Review HMIS records to ensure that the agency does not have previous violations
- Verify that the required documentation has been correctly executed and submitted or viewed on site, including:
  - Partner Agreement
  - Additional Documentation on Agency and Project(s)
  - Designation of HMIS Primary Agency Administrator
  - Fee Payment, if applicable
- Requests to set up a new agency in the HMIS are presented to the D&E Committee for informational purposes
- Work with the Partner Agency to input applicable agency and program information
- Work with the HMIS Lead/Administrator to migrate legacy data, if applicable

Agency Information Security Protocol Requirements

At a minimum, Partner Agencies must develop security rules, protocols or procedures based on the final *HUD Data and Technical Standards* including but not limited to the following:

- Internal agency procedures for complying with the HMIS Notice of Privacy Practices and provisions of other HMIS client and agency agreements
- Maintaining and posting an updated copy of the agency's Notice of Privacy Practices on the agency's website
- Posting a sign in the areas of client intake that explains generally the reasons for collecting personal information
- Appropriate assignment of user accounts
- Preventing user account sharing

- Protection of unattended workstations
- Protection of physical access to workstations where employees are accessing HMIS
- Safe storage and protected access to hardcopy and digitally generated client records and reports with identifiable client information
- Proper cleansing of equipment prior to transfer or disposal
- Procedures for regularly auditing compliance with the agency's information security protocol

The HMIS Lead/Administrator conducts annual site visits to monitor compliance with HMIS policies, at which time agencies may need to demonstrate their procedures for securing client data.

User Access Levels

All HMIS users must be assigned a designated user access level that controls the level and type of access the user will have within the system. Users will have access to client-level data that is collected only by their own agency unless a client specifically consents in writing to share their information. All Agency Administrators determine end user access levels.

Data Access Control Policies

User Accounts

Partner Agencies are responsible for managing user accounts following the procedures documented in the *HMIS User Implementation* section of this manual for user account set-up including verification of eligibility, the appropriate training, and the establishment of appropriate user type. The assigned user type will determine each user's individual access level to data, and Partner Agencies must regularly review user access privileges.

Partner Agencies are responsible for inactivating and/or removing users from the system by contacting the HMIS Lead/Administrator. They should discontinue the rights of a user immediately upon that user's termination from any position with access.

User Passwords

Each user will be assigned a unique identification code (User ID), the end-users work email.

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

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

Password Reset/Unsuccessful Login

Users can reset their own password directly from the login page. The HMIS Lead/Administrator and in some cases, the Agency Administrator, have the ability to

temporarily reset a password. If an Agency Administrator needs to have his/her password set, the HMIS Lead/Administrator will need to reset that password.

Temporary Suspension of User Access to HMIS

System Inactivity

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

Electronic Data Control

Agency Policies Restricting Access to Data

Partner agencies must establish protocols limiting internal access.

Downloaded Data

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

Ability to Export Agency-specific Data from the HMIS

Partner Agencies will have the ability to export a copy of their own data for internal analysis and use. Agencies are responsible for the security of this information.

Hardcopy Data Control

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

HMIS Privacy Plan

The Continuum has defined a privacy plan that includes:

- Data collection limitation
- Purpose and use limitations
- Allowable uses and disclosures
- Access and correction standards

- Protection for survivors of domestic violence, dating violence, sexual assault, and stalking
- Protections for clients engaged in substance abuse services

Data Collection Limitation Policy

Partner Agencies will solicit or enter information about clients into the HMIS database only in order to provide services or conduct evaluation or research. Partner Agency management, in consultation with the CoC, will make a determination of what qualifies as essential for services or research.

Client Notification Policies and Procedures

The CoC has prepared standard documents for HMIS Notice of Privacy Practices and Client Consent to Release Information which are available on the CoC web site (https://publicassistance.arlingtonva.us/10yp/). Partner Agencies may either use these forms or incorporate the content of the HMIS documents into the agency's own documentation. All written consent forms must be stored in a client's case management file for record keeping and auditing purposes.

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

Agencies that are recipients of federal assistance shall provide required information in languages other than English that are common in the community if speakers of these languages are found in significant numbers and come into frequent contact with the program.

The HMIS Lead/Administrator conducts annual site visits to monitor compliance with HMIS policies, at which time agencies may need to provide examples of the above-mentioned privacy documents and their procedures for protecting the privacy of client data.

Confidentiality protections set forth in VAWA apply to any survivor who (1) requests services (regardless if they are provided services or not), (2) is receiving services, or (3) has received services in the past.

Since it is possible to identify many victims in small communities with only ethnicity or age and zip code, the information that victim service providers can share must be carefully scrutinized and limited. In addition, non-personally identifying information must be further protected by being "de-identified, encrypted, or otherwise encoded."

Definitions and Descriptions of Client Notification and Consent Procedures

Client Notice

A written notice of the assumed functions of the HMIS must be posted and/or given to each client so that he/she is aware of the potential use of his/her information and where it is stored. No consent is required for the functions articulated in the notice. However, as part of the notification process, clients must be informed of their right to designate their client records as hidden/closed and to view a copy of his/her record upon request.

To fulfill this requirement, the agency may adopt the HMIS Notice of Privacy Practices, or develop an equivalent Privacy Notice that incorporates all of the content of the standard HMIS Notice. If the agency has a website, the adopted Notice of Privacy Practices or equivalent privacy notice must be posted on the website.

Hidden/Closed Client Record

After learning about the HMIS, if a client does not wish to have his/her Primary Identifiers accessible to all HMIS users, the originating HMIS user should enter the client anonymously. Creating the client record anonymously will allow the agency to access the client's information for agency purposes (see instructions below). This action will allow the Agency staff to view client-identifying information but will prevent any personal client-identifying information from being accessed by HMIS users outside of the originating agency.

Creating an Anonymous Client Requirements

- Enter Name as: Anonymous (HMIS Client ID), *Full Name Reported*
- Enter date of birth for months 1-6 as: 1/1/XXXX (actual year of birth), *Full DOB Reported*
- Enter date of birth for months 7-12 as: 7/1/XXXX (actual year of birth), *Full DOB Reported*
- Enter social security number as: 999-99-9999, *Full SSN Reported*

Written Client Consent for CoC Network Data Sharing

At the initial intake, the client should be provided an oral explanation and written documentation about the option of sharing his/her Information within the CoC HMIS. This documentation should also be provided annually, if a household is enrolled in a project on a long-term basis. If a client is willing to share his/her information within the HMIS, he/she must provide written consent (see exception below for call center operations). The consent must be specific regarding:

- Purpose
- The expiration of the sharing (not to exceed one year after being signed)
- Affected data elements
- Function
- Involved parties

The client maintains a right to revoke written authorization at any time (except if that policy is overridden by agency policy or if the information is required to be shared as a condition of a provider agreement). Note that any such revocation will not be retroactive to any information that has already been released. To fulfill this requirement, the client must submit in writing a request to revoke their consent for CoC network data sharing.

Client Authorization

HMIS users may share client information only if the client authorizes that sharing with a valid Client Release of Information form, or in the case of call center operations (i.e., 1010 hotline, DHS customer service, etc.), explicit oral consent.

Authorized users will be able to grant permission based on appropriate client consent to share individual client information with another agency's users. Random file checks for appropriate client authorization, audit trails, and other monitoring tools may be used to ensure that this data sharing procedure is followed. Specific monitoring procedures around program enrollment will be implemented to ensure appropriate client information access.

At any time clients have the right to opt-out. Survivors of domestic violence, dating violence, sexual assault or stalking have the right to decline having any information about them entered into an HMIS system, as well as the opportunity to decline any or all electronic HMIS entry regardless of whether the information is hidden or open.

Applicability of Consents

The Partner Agency shall uphold federal and state confidentiality regulations to protect client records and privacy. If an agency is covered by the Health Insurance Portability and Accountability Act (HIPAA), VAWA, HOPWA and 42CFR, the HIPAA regulations prevail. Consents are time-limited with a specific purpose.

HMIS Data Use and Disclosure Policies and Procedures

Each of the HMIS Partner Agencies must comply with the following uses and disclosures, as outlined in the *HUD Data and Technical Standards: Notice for Uses and Disclosures for Protected Personal Information (PPI)*. A Partner Agency has the right to establish additional uses and disclosures as long as they do not conflict with the CoC-approved uses and disclosures.

Privacy Notice Requirement

Each Partner Agency must publish a privacy notice that incorporates the content of the *HUD Data and Technical Standards Notice* as described below. Agencies that develop their own privacy and security policies must allow for the de-duplication of homeless clients at the Continuum level.

Each agency must post the privacy notice and provide a copy of the privacy notice to any client upon request.

An agency's privacy notice must:

- Specify all potential uses and disclosures of a client's personal information
- Specify the purpose for collecting the information
- Specify the time period for which a client's personal information will be retained at the agency
- Specify the method for disposing of a client's personal information or removing identifiers from personal information that is not in current use seven years after it was created or last changed

- State the process and applicability of amendments, and commit to documenting all privacy notice amendments
- Offer reasonable accommodations for persons with disabilities and/or language barriers throughout the data collection process
- Allow the individual the right to inspect and to have a copy of his/her client record and offer to explain any information that the individual may not understand, as outlined in the Arlington County CoC Client Bill of Rights
- Specify a procedure for accepting and considering questions or complaints about the privacy and security policies and practices

CoC – Approved Uses and Disclosures

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

Case management purposes include uses associated with providing or coordinating services for a client. As part of case management, the agency will share client information with other agencies based only on written client consent, or in the case of call center operations, explicit oral consent except when a client requests that his/her record remains anonymous. Additionally, a client receiving services from an agency whose primary mission is to provide services to victims of domestic violence, dating violence, sexual assault or stalking may request for information not to be shared.

- Administrative purposes are uses required to carry out administrative functions, including but not limited to legal, audit, personnel, oversight and management functions. An example would be analyzing client outcomes to evaluate program effectiveness
- Analytical purposes are functions that are related to analyzing client data to understand homelessness, including but not limited to creating de-identified protected personal information, understanding trends in homelessness and the needs of persons who are homeless, and assessing the implementation of the Continuum's 10-Year Plan to End Homelessness

Unless a client requests that his/her record remains anonymous, his/her primary identifiers will be disclosed to other HMIS agencies. This will allow agencies to locate the client within the HMIS system when the client comes to them for services. This will allow the CoC to determine how many people are experiencing homelessness in suburban Arlington County during any specified timeframe.

Identifiable client information may also be used, or disclosed, in accordance with the *HUD Data and Technical Standards* for:

- Uses and disclosures required by law
- Aversion of a serious threat to health or safety
- Uses and disclosures about survivorss of abuse, neglect or domestic violence
- Uses and disclosures for academic research purposes

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

Aside from the disclosures specified above, a client's protected personal information will be disclosed only with his/her written consent.

Client information will be stored with personal identifiers for a period of seven years from the time it was last modified. Beyond that point, client information will be retained only in a de-identified format.

HMIS Data Release Policies and Procedures

Client-identifying Data

No identifiable client data will be released to any person, agency, or organization for any purpose other than those specified in the *HMIS Data Use and Disclosure Policies and Procedures* section.

Data Release Criteria

HMIS client data will be released only in aggregate, or in anonymous client- level data formats, for any purpose beyond those specified in the *HMIS Data Use and Disclosure Policies and Procedures* section of this manual, such that the identity of any individual or household cannot be determined.

Parameters of the release of aggregate data (*i.e.*, where the data comes from, what it includes and what it does not include) will be presented to each requestor of aggregate data.

Data Release Process

Beyond individual agency reports, or CoC reports on its funded programs, the Executive Committee 10 Year Plan to End Homelessness in Arlington County must approve all data for public classification and release.

Specific Call Center Exception to Written Consent Requirement

Call center operations will not be required to obtain written consent to share primary and general client information collected primarily through telephonic or other electronic means. However, all clients must be informed of their rights regarding HMIS participation. Clients will be read the call center consent and notifications script. Clients can view the Privacy Notice on the CoC website or pick up a copy at the CoC office.

Specific Client Notification Procedures for Survivors of Domestic Violence, Dating Violence, Sexual Assault, and Stalking

A non-domestic violence provider agency that is serving a survivor of domestic violence, dating violence, sexual assault, or stalking must designate her/his record as anonymous to other agencies. Thus, the client notification form must clearly state the potential safety risks for domestic violence, dating violence, sexual assault or stalking survivors and delineate the information sharing options. All Partner Agency staff must be trained on the protocol for educating survivors about their individual information sharing

options. The CoC provides a sample Domestic Violence Notice as part of the Privacy Document Packet on the CoC website (https://publicassistance.arlingtonva.us/10yp/10-year-plan-committees/).

Specific Client Notification Procedures for Unaccompanied Minor Youth

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

Privacy Compliance and Grievance Policy

Partner Agencies must establish a regular process of training users on this policy, regularly auditing that the policy is being followed by agency staff (including employees, volunteers, affiliates, contractors and associates), and receiving and reviewing complaints about potential violations of the policy. Agency Administrators can monitor privacy compliance and oversee complaints.

HMIS Data Quality Plan

The Continuum has defined a data quality plan that:

- Based on HUD data standards and CoC data requirements, specifies the data quality standard to be used by all participating agencies
- Provides a mechanism for monitoring adherence to the standard
- Provides the necessary tools and training to ensure compliance with the standard
- Includes strategies for working with agencies that are not in compliance with the standard by providing technical support

HMIS Data Collection

Data Quality Standard

- All data entered will be accurate defined by collection and entry of data into the HMIS ensures that the data is the best possible representation of reality as it relates to homeless persons and the programs that provide homeless housing and services.
- Data in the HMIS should accurately reflect client data recorded in the client's file, along with information known about the client and the housing and/or services received by the client.
- Per HUD data standards, blank entries in required data fields will not exceed 5% per month
- All services provided will be compatible with providing program
- Data entry, including program Entry and Exit transactions, must be complete within 2 business days of data collection

Universal Data Element	Target	Acceptable NULL/Missing	Acceptable "Client doesn't know", "Client Refused"
Name	100%	0%	0%
Social Security Number	100%	0%	5%
Date of Birth	100%	0%	0%
Race	100%	0%	5%
Ethnicity	100%	0%	0%
Gender	100%	0%	5%
Veteran Status	100%	0%	0%
Disabling Condition	100%	0%	5%
Living Situation	100%	0%	0%
Project Entry Date	100%	0%	0%
Project Exit Date	100%	0%	0%
Destination	100%	0%	5%
Relationship to Head of Household	100%	0%	0%
Client Location	100%	0%	0%

Data Quality Monitoring

The HMIS Lead/Administrator will perform regular data integrity checks on the HMIS data. Any patterns of error at a Partner Agency will be reported to the Agency Administrator and/or Primary Point Person. When patterns of error have been discovered, users will be required to correct data entry techniques and will be monitored for compliance.

Partner Agency Administrators are expected to:

- Run Validation Reports per program on a monthly basis
- Notify Agency Staff of findings and timelines for correction
- Rerun reports for errant agencies/programs to confirm data correction
- Submit APRs on a quarterly/annual basis

Data Collection Requirements

Required Data Elements

A Partner Agency is responsible for ensuring that a minimum set of data elements, referred to as the Universal Data Elements (UDE's) and Program-specific Data Elements as defined by the *HUD Data and Technical Standards*, and other data elements as determined by the HMIS Committee, will be collected and/or verified from all clients at their initial program enrollment or as soon as possible thereafter. Partner Agencies are required to enter data into the HMIS within two business days of collecting the information.

These required data elements are all included collectively on the *Client Profile*, *Client Demographics* section, *Comprehensive Entry*, and *Interim and Review* assessments and includes timely entry of program Entry and Exit transaction data.

Partner Agencies must report client-level UDE's and Program-specific Data Elements using the required response categories detailed in the *HUD Data and Technical Standards.* These standards are already incorporated into the HMIS.

Entry/Exit Data

Program entry and exit dates should be recorded upon any program entry or exit on all participants. Entry dates should record the first day of service or program entry with a

new program entry date for each period/episode of service. Exit dates should record the last day of residence in a program's housing before the participant leaves the shelter or the last day a service was provided.

Data Quality Training Requirements

End-User Training

Each end user of the HMIS system must complete CoC approved HMIS training by the Agency Administrator before being given HMIS log-in credentials. It is recommended that the Agency Administrator identifies agency-specific nuances and how they enter data. HMIS Agency Administrators should notify the CoC when they have specific training needs for their end-users.

Reports Training

Reports training for Agency Administrators and other interested users will be made available as needed. These will include training on how to use Provider Reports in ETO, how to run existing reports in the ETO Reports, and may include opportunities for training in report creation using Business Objects. (Note: Use of Business Objects requires a separate Report Viewer or Ad-hoc Report Creation license).

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

HMIS De-duplication of Data - Policies and Procedures

User-mediated Look-up

The primary way to achieve de-duplication will be a user -mediated search of the client database prior to creating a new client record. The user will be prompted to enter a minimum number of the data elements into the HMIS application, and a list of similar client records will be displayed. Based on the results, the user will be asked to select a matching record if the other identifying fields match correctly.

If the user is unsure of a match (either because some data elements differ or because of blank information), the user should query the client for more information and continue evaluating possible matches or create a new client record.

The user will not be able to view sensitive client information or program -specific information during the de-duplication process. After the client record is selected, the user will be able to view previously existing portions of the client record only if he/she has explicit authorization to view that client's record.

De-duplicating Data Elements

The HMIS application will use the following data elements to create unduplicated client records:

- Name (first, middle, last, suffix; aliases or nicknames should be avoided)
- Social Security Number
- Date of Birth (actual or estimated)

- Gender
- Race and Ethnicity

Back-end Central Server Matching Based on Identifiable Information

When Primary Identifiers are not shared across agencies for de-duplication purposes, the HMIS Lead/Administrator with the assistance of the Agency Administrator will manage a process for matching a client's personal identifying information based on a unique client identifier that is assigned by the HMIS to each client. The unique client identifier provides an unduplicated internal count of clients served by the Agency and provides the HMIS Lead/Administrator the means of conducting longitudinal analysis of services provided to each client.

This scenario will be used to de-duplicate hidden client records. The process will also be used to validate data received from all users, as human decisions and misjudgments may introduce error to the provider-mediated look-up process.

TECHNICAL SUPPORT

HMIS TECHNICAL SUPPORT POLICIES AND PROCEDURES

HMIS Support

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

During the normal business hours of the CoC:

- ⇨ Begin with reviewing HMIS guidebook & training materials
- ⇨ If the question is still unresolved, then direct the technical support question to the Agency Administrator
- ⇨ If the question is still unresolved, the Agency Administrator can direct the question to the HMIS Lead/Administrator
- ⇨ If the question is still unresolved, the HMIS Lead/Administrator will direct the question to Social Solutions technical support staff

After the normal business hours of the CoC:

- ⇨ Begin with reviewing HMIS guidebook & training materials
- ⇨ If the question can wait to be addressed during the following business day, wait and follow the *normal business hours* outlined above
- ⇨ If the question cannot wait, direct the technical support question to the Agency Administrator

If it is determined that the issue needs immediate attention, the user's request will be forwarded to an appropriate Social Solutions HMIS technical support representative. Otherwise, the user will be instructed to pursue assistance through normal channels on the following business day.

If HMIS Lead/Administrator is unavailable beyond one week, you may contact the HMIS Support Team of Social Solutions at hmissupport@socialsolutions.com or 866-732-3560 ext. 2. Please send a copy of the issue to the HMIS Lead/Administrator.

User Training

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

Agency/User Forms

All Agency Administrators will be trained in the appropriate on-line and hardcopy forms. If the Agency Administrator has questions on how to complete HMIS forms, he/she shall contact the HMIS Lead/Administrator.

Report Generation

Each Agency may send its Agency Administrator to receive training on how to develop agency-specific reports using the HMIS application. The HMIS Lead/Administrator will be a resource to agency users as they develop reports but will be available to provide only a limited, reasonable level of support to each Agency.

The Data & Evaluation Committee will be the primary body to query Partner Agencies on their reporting needs and to prioritize a list of reports to be developed by the CoC for use by all Partner Agencies.

Programming-related Service Requests

If a user encounters programming issues within the HMIS application that need to be addressed, that user should identify the error or suggest an improvement to the Agency Administrator. The Agency Administrator will forward this information to the HMIS Lead/Administrator, identifying the specific nature of the issue or recommended improvement, along with the immediacy of the request.

The HMIS Lead/Administrator will review all application service requests and determine the action to be taken. Requests to fix programming errors will be prioritized and forwarded to Social Solutions. Suggested application improvements will be compiled and periodically discussed by the Data & Evaluation Committee. A prioritized list of improvements will be submitted to the HMIS Lead/Administrator for review. Approved recommendations will be submitted to Social Solutions.

HMIS System Availability Policies

There are times that ETO is unavailable because Social Solutions is performing necessary backup and maintenance of the HMIS database. These are usually in the late evenings when as few people as possible need access to the system. However, when the CoC receives notice of a planned interruption of service for other reasons or for an abnormal amount of time, the HMIS Lead/Administrator will notify Agency Administrators via email. If there is an unplanned interruption to service, the HMIS Lead/Administrator will communicate with Social Solutions and Agency Administrators will be notified of any information regarding the interruption as it is made available.

APPENDIX A: GLOSSARY OF HMIS ACRONYMS AND TERMS

Adapted from http://www.hmis.info/Resources/742/HMIS-Acronyms-and-Definitions.aspx

Acronyms

AIRS - CoC of Information & Referral Systems

AHAR - Annual Homeless Assessment Report

APR - Annual Performance Report

42CFR – Confidentiality of Alcohol and Drug Abuse Patient Records

CHO – Contributing HMIS Organization

CoC - Continuum of Care

DOB - Date of Birth

DV - Domestic Violence

ESG - Emergency Solutions Grants

ETO – Efforts to Outcomes

eHIC – electronic Housing Inventory Chart

FIPS - Federal Information Processing Standards Codes for states, counties, and named populated places.

HEARTH – Homeless Emergency Assistance and Rapid Transition to Housing

HIPAA - Health Insurance Portability and Accountability Act of 1996

HMIS - Homeless Management Information System

HOPWA – Housing Opportunities for Persons With AIDS

HUD - U.S. Department of Housing and Urban Development

I&R - Information and Referral

MH - Mental Health

NOFA - Notice of Funding Availability

PIT - Point in Time

PKI - Public Key Infrastructure

PPI - Personal Protected Information

S+C - Shelter Plus Care (McKinney-Vento Program)

SA - Substance Abuse

SHP - Supportive Housing Program

SRO - Single Room Occupancy

SSN - Social Security Number

SSI - Supplemental Security Income

SSO - Supportive Services Only

SSVF – Supportive Services for Veteran Families Program

TA - Technical Assistance

TANF - Temporary Assistance for Needy Families

VAWA - Violence Against Women Act

XML - Extensible Markup Language

Terms

CoC of Information and Referral Systems (AIRS)

The professional association for over 1,000 community information and referral (I&R) providers serving primarily the United States and Canada. AIRS maintains a taxonomy of human services.

Annual Performance Report (APR)

A report that tracks program progress and accomplishments in HUD`s competitive homeless assistance programs. The APR provides the grantee and HUD with information necessary to assess each grantee`s performance.

Audit Trail

A record showing who has accessed a computer system and what operations he or she has performed during a given period of time. Most database management systems include an audit trail component.

Bed Utilization

An indicator of whether shelter beds are occupied on a particular night or over a period of time.

Biometrics

Refers to the identification of a person by computerized images of a physical feature, usually a person’s fingerprint.

Chronic homelessness

HUD defines a chronically homeless person as a homeless individual with a disabling condition who has either been continuously homeless for a year or more OR has had at least four (4) episodes of homelessness in the past three (3) years. To be considered chronically homeless, persons must have been sleeping in a place not meant for human habitation (e.g., living on the streets) and/or in an emergency homeless shelter during

that time*. Persons under the age of 18 are not counted as chronically homeless individuals.*

Chronically Homeless Household

HUD defines a chronically household as a family that has at least one adult member (persons 18 or older) who has a disabling condition who has either been continuously homeless for a year or more OR has had at least four (4) episodes of homelessness in the past three (3) years. To be considered chronically homeless, persons must have been sleeping in a place not meant for human habitation (e.g., living on the streets) and/or in an emergency shelter/safe haven during that time.

Client Intake

The process of collecting client information upon entrance into a program.

Consumer

An individual or family who has experienced or is currently experiencing homelessness.

Continuum of Care (CoC)

A community with a unified plan to organize and deliver housing and services to meet the specific needs of people who are homeless as they move to stable housing and maximize self-sufficiency. HUD funds many homeless programs and HMIS implementations through Continuum of Care grants.

Coverage

A term commonly used by CoCs or homeless providers. It refers to the number of beds represented in an HMIS divided by the total number of beds available.

Contributing HMIS Organization (CHO)

Any organization (including its employees, volunteers, affiliates, contractors, and associates) that records, uses or processes data on homeless clients for an HMIS. The requirements of the HMIS Final Notice apply to all Contributing HMIS Organizations.

Data Quality

The accuracy and completeness of all information collected and reported to the HMIS.

Data Standards

See HMIS Data and Technical Standards Final Notice.

De-identification

The process of removing or altering data in a client record that could be used to identify the person. This technique allows research, training, or other non-clinical applications to use real data without violating client privacy.

Digital Certificate

An attachment to an electronic message used for security purposes. The most common use of a digital certificate is to verify that a user sending a message is who he or she claims to be and to provide the receiver with the means to encode a reply.

Disabling Condition

A disabling condition in reference to chronic homelessness is defined by HUD as a diagnosable substance use disorder, serious mental illness, developmental disability, or chronic physical illness or disability, including the co-occurrence of two or more of these conditions. A disabling condition limits an individual's ability to work or perform one or more activities of daily living.

Emergency Shelter

Any facility whose primary purpose is to provide temporary shelter for the homeless in general or for specific populations of the homeless.

Emergency Solutions Grant (ESG)

A federal grant program designed to help improve the quality of existing emergency shelters for the homeless, to make available additional shelters, to meet the costs of operating shelters, to provide essential social services to homeless individuals, and to help prevent homelessness.

Encryption

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

Final Notice

See HMIS Data and Technical Standards Final Notice.

Hashing

The process of producing hashed values for accessing data or for security. A hashed value is a number or series of numbers generated from input data. The hash is generated by a formula in such a way that it is extremely unlikely that some other text will produce the same hash value or that data can be converted back to the original text. Hashing is often used to check whether two texts are identical. For the purposes of Homeless Management Information Systems, it can be used to compare whether client records contain the same information without identifying the clients.

HEARTH Act

On May 20, 2009, President Obama signed the Homeless Emergency Assistance and Rapid Transition to Housing (HEARTH) Act of 2009. The HEARTH Act amends and reauthorizes the McKinney-Vento Homeless Assistance Act.

Homeless Management Information System (HMIS)

Computerized data collection tool designed to capture client- level information over time on the characteristics and service needs of men, women, and children experiencing homelessness.

HMIS Data and Technical Standards Final Notice

Regulations issued by HUD via the Federal Register describing the requirements for implementing HMIS. The *HMIS Final Notice* contains rules about who needs to participate in HMIS, what data to collect, and how to protect client information.

Housing Inventory Chart (HIC)

A calculation of the numbers of beds and housing units in a region on one particular night, usually coinciding with the annual Point-in-Time count.

Inferred Consent

Once clients receive an oral explanation of HMIS, consent is assumed for data entry into HMIS. The client must be a person of age, and in possession of all his/her faculties (for example, not mentally ill).

Informed Consent

A client is informed of options of participating in an HMIS system and then specifically asked to consent. The individual needs to be of age and in possession of all of his faculties (for example, not mentally ill), and his/her judgment not impaired at the time of consenting (by sleep, illness, intoxication, alcohol, drugs or other health problems, etc.).

Information and Referral

A process for obtaining information about programs and services available and linking individuals to these services. These services can include emergency food pantries, rental assistance, public health clinics, childcare resources, support groups, legal aid, and a variety of non-profit and governmental agencies. An HMIS usually includes features to facilitate information and referral.

McKinney-Vento Act

The McKinney- Vento Homeless Assistance Act was signed into law by President Ronald Reagan on July 22, 1987. The McKinney-Vento Act funds numerous programs providing a range of services to homeless people, including the Continuum of Care Programs: the Supportive Housing Program, the Shelter Plus Care Program, and the Single Room Occupancy Program, as well as the Emergency Solutions Grant Program.

Notice of Funding Availability (NOFA)

An announcement of funding available for a particular program or activity.

Penetration Testing

The process of probing a computer system with the goal of identifying security vulnerabilities in a network and the extent to which outside parties might exploit them.

Permanent Supportive Housing

Long term, community based housing that has supportive services for homeless persons with disabilities. This type of supportive housing enables special needs populations to live as independently as possible in a permanent setting. Permanent housing can be provided

in one structure or in several structures at one site or in multiple structures at scattered sites.

Point in Time Count

A snapshot of the homeless population taken on a given day. Since 2005, HUD requires all CoC applicants to complete this count every other year in the last week of January. This count includes a street count in addition to a count of all clients in emergency and transitional beds.

Privacy Notice

A written, public statement of an agency's privacy practices. A notice informs clients of how personal information is used and disclosed. According to the *HMIS Data and Technical Standards*, all covered homeless organizations must have a privacy notice.

Program-specific Data Elements

Data elements required for programs that receive funding under the McKinney-Vento Homeless Assistance Act and complete the Annual Performance Reports (APRs).

Public Keys

Public keys are included in digital certificates and contain information that a sender can use to encrypt information such that only a particular key can read it. The recipient can also verify the identity of the sender through the sender`s public key.

Scan Cards

Some communities use ID cards with bar codes to reduce intake time by electronically scanning ID cards to register clients in a bed for a night. These ID cards are commonly referred to as scan cards.

Single Room Occupancy (SRO)

A residential property that includes multiple single room dwelling units. Each unit is for occupancy by a single eligible individual. The unit need not, but may, contain food preparation or sanitary facilities, or both. It provides rental assistance on behalf of homeless individuals in connection with moderate rehabilitation of SRO dwellings.

Shelter Plus Care Program

A program that provides grants for rental assistance for homeless persons with disabilities through four component programs: Tenant, Sponsor, Project, and Single Room Occupancy (SRO) Rental Assistance.

Supportive Housing Program

A program that provides housing, including housing units and group quarters, that has a supportive environment and includes a planned service component.

Supportive Services

Services that may assist homeless participants in the transition from the streets or shelters into permanent or permanent supportive housing, and that assist persons with living successfully in housing.

Transitional Housing

A project that has as its purpose facilitating the movement of homeless individuals and families to permanent housing within a reasonable amount of time (usually 24 months).

Unduplicated Count

The number of people who are homeless within a specified location and time period. An unduplicated count ensures that individuals are counted only once regardless of the number of times they entered or exited the homeless system or the number of programs in which they participated. Congress directed HUD to develop a strategy for data collection on homelessness so that an unduplicated count of the homeless at the local level could be produced.

Universal Data Elements

Data required to be collected from all clients serviced by homeless assistance programs using an HMIS. These data elements include date of birth, gender, race, ethnicity, veteran's status, and Social Security Number (SSN). These elements are needed for CoCs to understand the basic dynamics of homelessness in their community and for HUD to meet the Congressional directive.

Written Consent

Written consent embodies the element of informed consent in a written form. A client completes and signs a form documenting the client's understanding of the options and risks of participating or sharing data in an HMIS system and consenting to such participation and data sharing. The signed document is then kept on file at the agency.