McHenry County Continuum to End Homelessness
Homeless Management Information System (HMIS)

McHenry County
HMIS
Policies and Procedures Manual

TABLE OF CONTENTS

BY-LAWS
OF
The McHenry County Continuum of Care to End Homelessness

DATE LAST MODIFIED: JANUARY 16, 2014
DATE CREATED: JUNE 25, 2012 *(Note: Portions were adapted from: "McHenry County Continuum of Care: Rules and Procedures", Adopted March 27, 2003 with subsequent revisions made on March 24, 2005 and February 15, 2007.)*

Article 16. HMIS (Homeless Management Information System)

Recognizing that a Homeless Management Information System (HMIS) is the information system designated by the CoC to comply with the requirements of the CoC Program interim rule at 24 CFR 578, other requirements established by HUD, including the 2014 HMIS Data Standards Manual, and any local requirements, the McHenry County CoC will designate an eligible agency, to be known as the HMIS Lead, to manage its HMIS. The HMIS Lead, in consultation with the CoC, Collaborative Applicant and HMIS Advisory Committee, will also be responsible for developing all the policies and procedures necessary for compliance with the CoC Program interim rule, the 2010 HMIS Data Standards, and any local requirements. These policies and procedures will be incorporated into the McHenry County CoC governance charter by reference, will be available upon request, and will include the following provisions:

- is updated annually;
- includes all policies and procedures necessary to comply with the HMIS requirements in the CoC Program interim rule, the 2014 HMIS Data Standards, and any local HMIS requirements;
- clearly outlines the roles and responsibilities of the CoC and HMIS Lead, and;
- includes the following plans:
    - Privacy Plan: A plan that at the minimum includes data collection limitations; purpose and use limitations; allowable uses and disclosures; access and correction standards; and protections for victims of domestic violence, dating violence, sexual assault, and stalking
    - Security Plan: A plan that ensures the confidentiality, integrity, and availability of all HMIS information; protects against any reasonably anticipated threats or hazards to security, and ensure compliance by end users.
    - Data Quality Plan: A plan that ensures completeness, accuracy, and consistency of the data in the HMIS.

CONTACT INFORMATION

MCHENRY COUNTY DEPARTMENT OF PLANNING AND DEVELOPMENT

Dennis Sandquist AICP, Director, DASandquist@co.mchenry.il.us
Jeffrey Harris, AICP, Community Development Administrator
Faith Taylor, Community Development Specialist
Kim Ulbrich, Community Development Specialist
Dave Watkins, Procurement Officer/Inspector
Lynnsey Obsorne, Administrative Specialist
McHenry County Government Center, Administration Building
667 Ware Road, Woodstock, IL 60098 815-334-4560

MCHENRY COUNTY MENTAL HEALTH BOARD

620 Dakota St, Crystal Lake, IL 60014 815-455-2828

MCHENRY COUNTY CONTINUUM OF CARE

Chair: Hans Mach, Home of the Sparrow, 815-271-5444, hmach@HOSparrow.org
Co-Chair: Art Krzyzanowski, Thresholds, 815-338-8324, arthur.krzyzanowski@thresholds.org
Co-Chair: David Esposito, Thresholds, 815-338-8324, david.esposito@thresholds.org

HMIS LEAD AGENCY

Pioneer Center for Human Services
4100 Veterans Parkway
McHenry, IL 60050
815-759-7110 (switchboard)
Fax: 815-344-3815

Data Entry/Report Creation/Trouble Shooting
Karen Bloomdahl, HMIS Database Specialist
815-789-7220
kbloomdahl@pioneercenter.org

Non Technical/Policy and Procedures
Tom Riley, Grants Coordinator/HMIS Database Supervisor
815-759-7121
triley@pioneercenter.org

KEY SUPPORT ROLES AND RESPONSIBILITIES

There are different roles involved in operating an effective HMIS. Roles and responsibilities are different for the following entities: CoC, HMIS Lead Agency, and participating projects/agencies.

McHenry County Continuum of Care (CoC)

The CoC is a group composed of representatives from organizations including nonprofit homeless providers, victim service providers, faith-based organizations, governments, business, advocates, public housing agencies, school districts, social service providers, mental health agencies, hospitals, universities, affordable housing developers, law enforcement, organizations that serve veterans, and homeless and formerly homeless persons organized to carry out the responsibilities of the CoC.

The CoC provides:

1. HMIS Oversight.
    - Designate an official HMIS software.
    - Designate an HMIS Lead agency.
    - HMIS Standards Compliance (including maintaining documented evidencing of compliance)
2. Executes the HMIS Governance Agreement.
    - The HMIS Governance Agreement is a written agreement between CoC Lead with the HMIS Lead Agency, specifying functions and responsibilities of the HMIS Lead Agency.
    - Define the responsibilities for management of HMIS.
    - Define rights, obligations, timeliness, and transition procedures for HMIS governance, software, and data, in the event that the agreement is terminated.
    - The Governance Agreement includes a Participation Agreement requiring agencies to comply and sanctions for failure to comply.
    - Update and/or review the HMIS Governance Agreement annually.

HMIS Lead Agency

The HMIS Lead Agency is the entity designated by the Continuum of Care in accordance with 24 CFR part 580 to operate the Continuum's HMIS on the Continuum's behalf.

The HMIS Lead Agency:

1. Establishes HMIS.
2. Administers the day-to-day operational functions of operating and oversight of the HMIS.
3. Ensures consistent participation by agencies.
2. Develops and submits local HMIS policies and procedures.
    - HMIS Operational Policy & Procedures
    - Data Quality Plan

- Security Plan
- Privacy Plan

3. Updates and reviews HMIS Policy & Procedures annually.
4. Executes HMIS participation and end user agreements.
5. Execute a written HMIS participation Agreement with each agency.
6. Monitors compliance with applicable HMIS standards and HUD requirements.
7. Takes corrective action when needed.
8. Administers vendor agreements/contracts.
9. Conducts unduplicated accounting of homelessness on a monthly basis.
10. Acts as a liaison between the CoC and regional and national HMIS related organizations and participate in related activities.
11. Provides training and support to agency users.
12. Provides continuing quality improvement via data analysis and knowledge of best practices.
13. Provides required data/answers for the HUD Housing Assistance applications.
14. Generates HUD reports (Annual Housing Assessment Report (AHAR), Point In Time (PIT) Count for shelters only and Housing Inventory Count (HIC).
15. Be a CoC liaison for HMIS.
16. Does annual security review of itself and agencies.

Providers/Agencies Role:

1. Providers/Agencies are responsible for all activity associated with agency staff and use of the HMIS.
    - CoC Participation.
    - HMIS Participation.
    - Privacy and Security Compliance.
    - HMIS Policy and Procedure Compliance.
    - Data Quality Compliance.
    - Community Planning/Use of Data.
2. CoC Participation
    - Attend/Participate regularly CoC meetings and workshops.
    - Represent your homeless population in planning process.
    - Increase awareness of homeless needs.
    - Identify awareness of homeless needs.
    - Identify additional resources for homeless.
3. HMIS Participation and Governance
    - HMIS Agency Participation Agreement.
    - HMIS User License Agreement.
    - Client Consent/Release of information (ROI).
4. Privacy and Security Compliance
    - Know HMIS Privacy and Security Requirements.
    - Communicate HMIS Privacy and Security requirements to data custodians and system users.
    - Monitor regularly for compliance.

5. HMIS Policy and Procedure Compliance
    - Establish business controls and practices to ensure compliance to HMIS policies.
    - Communicate HMIS policy and procedure requirements to data custodians and system users.
    - Monitor compliance and periodically review business controls and practices for effectiveness.
6. Data Quality Compliance
    - Know Data Quality expectations for timeliness, completeness, and accuracy.
    - Communicate Data Quality expectations to data custodians and end users.
    - Monitor for compliance.
    - Provide incentives; enforce policies.
7. Community Planning/Use of Data
    - Provide quality data for community planning.
    - Actively participate in planning process.
    - Participate in Point In Time and Housing Inventory Processes.

McHenry County Department of Planning and Development:

1. Submission of the HUD Housing Assistance application.
2. CoC (includes HMIS) Planning and Administrative Support

McHenry County Mental Health Board

1. HMIS funding support
2. CoC (includes HMIS) Planning and Administrative Support

HMIS Operations & Security

Recognizing the importance of community efforts to capture better data, in 2001 Congress directed HUD on the need for data and analysis on the extent and nature of homelessness and the effectiveness of the McKinney-Vento Act Programs including:

- Developing unduplicated counts of clients served at the local level.
- Analyzing patterns of use of people entering and exiting the homeless assistance system.
- Evaluating the effectiveness of these systems.

HMIS became an eligible activity under 2001 SuperNOFA.
The HMIS of the McHenry CoC is ServicePoint®.

HMIS PARTICIPATION

1. Participation Requirements

- *Mandated Participation*

All projects that are authorized under HUD's McKenney-Vento Act as amended by the HEARTH Act to provide homeless services and grantees receiving assistance for Homeless Prevention and Rapid Re-housing projects under the American Recovery and Reinvestment Act of 2009 must meet the minimum HMIS participation standards as defined by this Policies and Procedures manual. These participating agencies will be required to comply with the applicable operating procedures and must agree to execute and comply with an HMIS Agency Partner Agreement.

- *Voluntary Participation*

Although funded agencies are required to meet only minimum participation standards, the CoC strongly encourages funded agencies to fully participate with all of their homeless projects.

While the CoC cannot require non-funded providers to participate in the HMIS, the CoC works closely with the non-funded agencies to articulate the benefits of the HMIS and to strongly encourage their participation in order to achieve a comprehensive and accurate understanding of homelessness in McHenry County.

2. Minimum Participation Standards

- Collect the Universal Data Elements (UDEs), as defined by HUD, for all clients served by projects participating in HMIS. Includes Entry Date and Exit Dates.
- Collect Program Specific Data Elements, as defined by HUD, for all clients served by projects mandated to participate in HMIS.
- Enter client-level data into the HMIS within fifteen working days after the start of the month of client interaction. Based on a survey sent to users.
- Comply with all HUD regulations for HMIS participation.

The CoC uses all submitted data for analytic and administrative purposes, including the preparation of CoC reports to funders and the CoC's participation in the Federal Annual Homeless Assessment Report (AHAR).

3. Participation Expectations

Authorized agency users directly enter client-level data into the HMIS database. Users have rights to access data for clients served by their agency The agency's data are stored in the HMIS central database server, which is protected by numerous technologies to prevent access from unauthorized users. Primary client identifiers (e.g. name, SSN, DOB and gender) will be available by query for HMIS users from partner agencies to prevent the duplication of client records in the database.

CONNECTIVITY AND COMPUTER SECURITY REQUIREMENTS

1. Internet Connectivity

- Agencies must have Internet connectivity for each workstation accessing the HMIS.

2. Web Browsers

- ServicePoint® is designed to be compatible with the newest versions of Internet Explorer, Mozilla Firefox, and Google Chrome.

3. Security Hardware/Software

- All workstations accessing the HMIS need to be protected by a 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. Hard copies containing client information generated by, or, for HMIS must be supervised at all times in a public area. When staff are not present, hard copies must be stored in a secure location.

4. Physical Security

- Providers must have locking doors, an intrusion-detection system and physical firewalls. Computers must have locking screen savers.

5. Disaster Protection and Recovery

- Provided by the CoC vendor, ServicePoint®. (Securing Client Data by Bowman System v.03.29.06. Includes protocols for communication with HMIS Lead, who would contact user agencies.)

6. Encryption

- Provided by the COC vendor, ServicePoint®. (Securing Client Data by Bowman System v.03.29.06.)

7. **Electric Data Storage**
   - Provided by the COC vendor, ServicePoint™. (Securing Client Data by Bowman System v.03.29.06.)

8. **Disposal**
   - Provided by the COC vendor, ServicePoint™. (Securing Client Data by Bowman System v.03.29.06.)

HMIS USER IMPLEMENTATION

- **Eligible Users**
  Each Provider 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, and the use of canned reports.

- **User Requirements**
  Prior to being granted a username and password, users must sign an HMIS End User Agreement that acknowledges receipt of a copy of the HMIS Policy and Procedures Manual pledges to comply with the manual.

  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 that are described within this Policies and Procedures manual. They are accountable for their actions and for any actions undertaken with their user name and password.

  The HMIS Lead Agency must ensure that users have received adequate training prior to being given access to the database. Each user will be trained yearly on data security, privacy, and quality.

- **Setting Up a New User.**
  The HMIS Lead must:
  1. Have the new user sign the User Participation Agreement.
  2. Verify that appropriate and sufficient training has been successfully completed.
  3. Create the new user ID and password in ServicePoint®.

  Once the user ID is established, the HMIS Lead is responsible for maintaining the user account. If any users leaves the agency or no longer needs access to the HMIS, the Provider must notify the HMIS Lead who will immediately terminate user access by deleting or inactivating the user account.

ENFORCEMENT MECHANISMS

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

Sanctions includes, but not are limited to:

1. Suspension of system privileges.
2. Revocation of system privileges.

All violations will be reported to the CoC Board within 5 days. Sanctions will be determined by the CoC Board.

An agency's access may also be suspended or revoked if serious or repeated violation(s) of the HMIS Policy and Procedures occur by the agencies' users.

AGENCY INFORMATION SECURITY PROTOCOL REQUIREMENTS

Agencies must:

1. Comply with the HMIS Notice of Privacy and Practices and provisions of other HMIS client and agency agreements.
2. Maintain and post an updated copy of the Notice of Privacy Practices. If the Provider has a website, the Notice should be posted on their website.
3. Prevent user account sharing.
4. Protect unattended workstations.
5. Protect the physical access to workstations where employees are accessing HMIS.
6. Safely store and protect access to hardcopy and digitally generated client records and reports and identifiable client information.
7. Conduct workforce security screenings.
8. Protect passwords by not storing or displaying them in any publicly accessible location.

The HMIS Lead will monitor security once a year of all HMIS user agencies and itself.

HMIS Client Data Privacy

Privacy and security applies to all agencies and projects that use, or process Personal Protected Information (PPI) for HMIS including CoC, homeless service provider, HMIS host or provider, etc. Employees, volunteers, affiliates, contractors, and associates are covered by the privacy standards of the agencies they deal with. Privacy and security standards apply to all agencies- regardless of funding source – who use HMIS. The Health Insurance Portability and Accountability Act (HIPAA) privacy rules take precedence over HMIS Privacy Standards. HIPAA covered entities are required to meet HIPAA baseline privacy requirements, not HMIS.

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. The client also has a right to view a copy of his/her record upon request. To fulfill this requirement, the agency may either adopt the "HMIS Notice of Privacy Practices" or may develop an equivalent privacy notice that incorporates all of the content of the standard HMIS Notice. The Client Notice must be posted at each Intake desk.

WRITTEN CLIENT CONSENT FOR COC DATA SHARING

At the initial intake, the client should be provided with an oral explanation and written documentation about the option of sharing his/her information within the HMIS.

The client maintains a right to revoke written authorization at any time, in which case, any currently shared information will become non-shared from that point forward. Each agency should have their own Client Revocation Form that is to be signed by the client. Each agency must have their own procedure for accepting complaints about privacy and security.

HMIS users may share client information only if the client authorizes that sharing with a valid Client Release of Information form. If the client refuses to sign, a written explanation for the reason of denial must be provided.

APPLICABILITY OF CONSENTS

The 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), the HIPAA regulations prevail.

The HMIS Lead has prepared standard documents for HMIS Notice of Privacy Practices and Client Consent to Release Information (ROI). Providers may either use these forms or incorporate the content of HMIS documents into the Provider's own documentation.

All written consent forms must be stored in a client's case management file for record keeping and auditing purposes.

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

Agencies shall provide reasonable accommodations for persons with disabilities throughout the data collection process. This may include, be limited to, providing qualified sign language interpreters, readers or materials in accessible forms such as Braille, audio, or large type, as needed by individual with a disability.

VICTIM SERVICE PROVIDER DATA IN HMIS

Victim service providers that are funded under HUD's Supportive Housing Program, Shelter Plus Care Program, Section 8 Moderate Rehabilitation SRO Program, Emergency Solutions Grant Program, and Continuum of Care Program are prohibited from disclosing any personally identifying information for purpose of HMIS, per the requirements of the Violence and Women and Department of Justice Reauthorization Act of 2005.

HMIS DATA QUALITY

Data quality is critical for a CoC to: (1) Measuring the nature and extent homelessness, (2) completing required HUD reports, (3) meet the CoC's local homeless data needs. Timely, accurate and complete is central and critical to success of HMIS. The data quality standards are to be reviewed/revised yearly.

HMIS DATA QUALITY PLAN

1. Specifies that data quality standard to be used by all participating agencies.
2. Provide a mechanism for monitoring adherence to the standard.
3. Provides the necessary tools and training to ensure compliance with the standard.
4. Includes strategies for working with agencies that are not in compliance with the standard.

DATA QUALITY STANDARDS

1. All names will be accurate.
2. Blank entries in required fields will not exceed 5% per month.
3. Data entry must be complete within fifteen working days after the beginning of the month of data collection.
4. Project entry and exit dates should be recorded upon any project entry or exit on all participants. Entry dates should record the first day of housing or project entry (for Services Only projects) with a new entry date for each period/episode of housing or service. Exit dates should record the last day of residence in a project's housing before the participant leaves housing or the last day a service was provided.

DATA QUALITY MONITORING

The HMIS Lead will perform regular data integrity reports on the HMIS data.

HMIS Lead will:

1. Run Data Quality Completeness Report Card [ART report 0252] monthly.
2. Run Duplicate Clients [0212] monthly.
3. Run other data quality reports as appropriate.
4. Rerun reports for errant Providers.

DATA COLLECTION REQUIREMENTS

Each agency is responsible for ensuring minimum set of data elements, referred to as the Universal Data Elements (UDE's) as defined by the *HUD Data and*

Technical Standards, will be collected and/or verified from all the clients at their initial project enrollment or as soon as possible thereafter. Providers are required to enter data into the HMIS fifteen working days after the beginning of the month of collecting information.

Agencies must provide client-level data for the Program-Specific Data Elements (PSDE) using the required response categories detailed in the "Required Response Categories for Program-specific Data Elements" section of the *HUD Data and Technical Standards.* These standards are already incorporated into the HMIS.

Income and disability elements are to be reviewed/updated quarterly.

Project Descriptor Data Elements (PDDE) are to be reviewed/updated every October.

Project Inventory is to be reviewed/updated at the time of the yearly HIC and PIT.

DATA QUALITY TRAINING

Each end user of the HMIS system must complete at least one training session with the HMIS Lead and sign the User License Agreement before being given HMIS login credentials. This includes basic data entry and running reports in ART (Advanced Reporting Tool).

All staff are encouraged to run their own data quality reports so that agencies can monitor their own data quality and become more effective in serving our clients across the Continuum.

Required HUD Annual Performance Reports (APRs) data will be entered by the Providers. Each provider will designate a person to enter the data into ***e-snaps***.

HMIS DATA ACCESS CONTROL POLICY

1. User Accounts

The HMIS Lead is responsible for managing user accounts for the agencies.
The HMIS Lead is responsible for inactivating and/or removing users from the system when contacted by the agency. He/she should discontinue the rights of a user immediately upon that user's termination from any position with access.

2. User Passwords

Each user will be assigned a unique identification code (User ID), preferably the first initial and last name of the user.
The user will be required to establish a new password upon their initial log-in. This password will need to be changed every 45 days. Passwords should be

between 8 and 16 characters long and contain at least two numbers. The password format is alphanumeric and case-sensitive.

3. Password Reset
Except when prompted by ServicePoint® to change an expired password, users cannot reset their own password. If a user needs to have his/her password set, the HMIS Lead will need to reset the password.

4. System Inactivity
Users must log off from the HMIS application and their workstation if they leave the workstation. Also, HUD requires password protected screen-savers on each workstation. If the user is logged onto a workstation and the period of inactivity on that workstation exceeds 30 minutes, the user will be logged off the system and/or will be asked if they wish to continue the session. (ServicePoint®.)

5. Unsuccessful Login
If a user attempts to log in 3 times unsuccessfully, the User ID will be "locked out", their access permission will be revoked, and they will be unable to regain access until their User ID is reactivated by the HMIS Lead. (ServicePoint®.)

6. Hardcopy Data Control
Printed versions (hardcopy) of confidential data should not be copied or left unattended and open to compromise. HMIS information in hardcopy format should be disposed of properly. This could include shredding finely enough to ensure that the information is unrecoverable.

HMIS DE-DUPLICATION OF DATA POLICY AND PROCEDURES

3. De-duplication of 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.
- Race and Ethnicity.

4. User mediated Look-up
The primary way to achieve de-duplication will be a user-mediated search for 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 the 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.

HMIS DATA USE AND DISCLOSURE POLICY AND PROCEDURE

CoC approved Uses and Disclosures

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

- Uses and disclosures by law.
- Aversion of a serious threat to health and safety.
- Uses and disclosures about victims of abuse, neglect or domestic violence.
- Uses and discloses for academic research purposes.
- Disclosures for law enforcement purposes in response to a lawful court order, court ordered warrant, subpoena or summons issued by judicial office or a grand jury subpoena.

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

HMIS DATA RELEASE POLICY AND PROCEDURES

1. Client-identifying Data

No identifiable client data will be released to any person, provider, or organization that is not the owner of said data for any purpose other than those specified in the *HUD Data Uses and Disclosure Policies and Procedures* section without the written permission of the client.

2. Data Release Criteria

HMIS client data will be released only in aggregate for the purpose beyond those specified in the *HUD Data Uses and Disclosure Policies and Procedures* section, according to the criteria specified below.

All data must be anonymous, be removal of either identifiers and/or all information that could be used to infer an individual or housed identity.

Only agencies can authorize release of aggregate program-specific information beyond the standard reports complied by the HMIS Lead for funding purposes. There will be full access to aggregate data for all participating agencies.

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.

Released aggregate data will be made available in the form of an aggregate report and/or raw dataset.

HMIS Technical Support Policies and Procedures

HMIS Application Support

As unanticipated technical support questions on the use of the HMIS application rise, user will follow the procedure to resolve those questions:

- Begin with utilization of training materials.
- If the question is still unresolved, direct the technical support question to the HMIS Lead.
- If the question is still unresolved, the System Administrator will direct the question to Bowman Systems support staff

User Training

The HMIS Lead will provide HMIS application training periodically throughout the year. If additional or specific training needs arise, the HMIS Lead may arrange for special training sessions. Agencies receiving HUD funding are required to be trained once a year. Yearly training includes data security, privacy and quality.

If users are entering data for an agency in a location that us out of the county, they can be trained by other CoCs in Illinois that use ServicePoint ®.

DEFINITIONS

Act: means the McKinney-Vento Homeless Assistance Act, and, unless otherwise specified, as amended by the Homeless Emergency Assistance and Rapid Transition to Housing Act of 2009 (HEARTH).

Continuum of Care (CoC): The group composed of representatives from organizations including nonprofit homeless providers, victim service providers, faith-based organizations, governments, business, advocates, public housing agencies, school districts, social service providers, mental health agencies, hospitals, universities, affordable housing developers, law enforcement, organizations that serve veterans, and homeless and formerly homeless persons organized to carry out the responsibilities of the CoC.

HIPPA: Health Insurance Portability and Accountability Act

HMIS: Homeless Management Information System. The information system designated by the Continuum of Care to comply with requirements of 24 CFR Part 580 and used to record, analyze data in regard to the provision of shelter, housing, and services to individuals and families who are homeless or at risk of homelessness.

HMIS Lead: The entity designated by the Continuum of Care in accordance with 24 CFR Part 580 to operate the Continuum's HMIS on the Continuum's behalf.

HMIS Vender: A contractor who provides materials or services for the operation of the HMIS. An HMIS vendor includes an HMIS software provider, web host server, as well as a provider of other technology or support.

HUD: Department of Housing and Urban Development.

Program: The federal funding source (e.g., HUD CoC).

Project: A distinct unit of an organization that provides services and/or lodging and is identified by the CoC as part of its service system.

Protected Identifying Information (PII): Information about a project participant that can be used to distinguish or trace a project participant's identity, either alone or when combined with other personal information, using methods reasonably likely to be used, which is linkable to the project participant.

Unduplicated count of homeless persons: An enumeration of homeless persons where each person is counted only once during a defined period.

User: An individual who uses or enters data into the HMIS.

Victim Service Provider: A private nonprofit organization whose primary mission is to provide services to domestic violence, dating violence, sexual assault, or stalking. The term includes rape crisis centers, battered women's shelters, domestic violence transitional housing projects, and other projects.

HMIS FORMS & REVIEW NOTES

Agency Participation Agreement (see User License Agreement)

Client Data Privacy Plan: (included in HMIS Policies and Procedures)

Data Quality Plan: (included in HMIS Policies and Procedures)

HMIS Policy and Procedures:
Last modified: 4/9/15
Last Annual Review/Approval by CoC: 12/11/2014
First Draft/Approval by CoC: 01/10/2013

Notice of Privacy Practices:
Reviewed/Approved by CoC: 6/13/13

Release of Information:
Reviewed/Approved by CoC: 7/13/13

Security Plan: (included in HMIS Policies and Procedures)

User License Agreement:
Reviewed/Approved by CoC: 5/8/2014