DUPAGE COUNTY HMIS STANDARD OPERATING PROCEDURE

Last Reviewed: 2/21/2024

The mission of the HMIS Team is to provide visionary data leadership by providing an effective and usable case management tool and by collecting and analyzing client and program-level data to report on the extent and nature of homelessness.

Table of Contents

Section 1: Introduction & Responsibilities

Introduction

The Homeless Management Information System (HMIS) is a database platform designed to capture uniform client information over time. This system is essential to efforts to streamline client services and inform public policy. Through HMIS, clients benefit from improved coordination in and between Participating Agencies within their respective Continuum of Care (CoC), informed advocacy efforts, and policies that result in targeted services. Analysis of information gathered by HMIS is critical to accurately calculate the size, characteristics, and needs of homeless and at-risk populations; data necessary to serve clients appropriately and for systems planning and advocacy.

Agencies who receive funding through the following federal partners and their respective programs are to participate in their local HMIS: U.S. Department of Health and Human Services, U.S. Department of Housing and Urban Development, U.S. Department of Veteran Affairs, and any additional funding source requiring participation. Victim Service Providers must utilize a comparable HMIS that meets all minimum privacy, security, and data requirements as set forth in these standard operating procedures.

DuPage County Community Services is the designated HMIS Lead which participates in the Northeast Illinois HMIS (NIL HMIS). The NIL HMIS is a shared, regional HMIS in which multiple CoC's participate, and is managed by a single Technical Lead Agency, the Alliance to End Homelessness in Suburban Cook County. The NIL HMIS is Governed through a separate Memorandum of Understanding and Administration and Communication Plans.

This document provides policies and procedures for partnering agencies and users under the DuPage County Continuum of Care. These policies and procedures are collectively referred to as the Standard Operating Procedures (SOP). The SOP have been developed to comply with HUD regulations, state and federal laws, meet local service coordination and reporting needs, and to retain consistency in developing and maintaining the HMIS.

The DuPage County CoC Data & Performance Committee is responsible for reviewing the SOP annually and proposing changes for approval by the DuPage County CoC Leadership Committee.

Roles and Responsibilities

The following documents outline the various roles and responsibilities as they relate to the DuPage County Continuum of Care Homeless Management Information System, in addition to the policies and procedures as outlined in the Standard Operating Procedures. These documents are available on the HMIS website, dupagehomeless.org/hmis/forms.

Document Title	Description
Memorandum of Understanding between the DuPage County Continuum of Care and DuPage County Department of Community Services	This document outlines the regional governing structure of the HMIS including the regional governing forum, the HMIS technical lead agencies, local CoCs, and local HMIS Leads.
Memorandum of Understanding between the DuPage County Continuum of Care and DuPage County Department of Community Services	This document designates the DuPage County Department of Community Services as the HMIS Lead and describes its responsibilities as such.
HMIS Partner Agreement between DuPage County Community Services and the Participating Agency	This document describes the responsibilities of HMIS participating agencies and their users.
HMIS Agency Data Administrator Policy and Code of Ethics	This document describes the responsibilities of HMIS participating agencies and their users.
HMIS End User Policy and Code of Ethics	This agreement describes the responsibilities and code of ethics by which each HMIS user must abide.
NIL HMIS System Administrator Plan	Outlines the NIL HMIS roles and requirements as they apply to local policies and procedures and management of the HMIS.

HMIS Partner Agreement between
DuPage County Community Services
and
____

This agreement is entered into on ________________(MM/DD/YY) between DuPage County Community Services, hereafter known as "HMIS LEAD" and ______________________________________ (agency name), hereafter known as "AGENCY," regarding access and use of the Homeless Management Information System, hereafter known as "HMIS."

I. Introduction

The HMIS, a shared human services database, allows authorized personnel at homeless and human service provider agencies throughout DuPage and Suburban Cook Counties Continuum of Care, to enter, track, and report on information concerning their own clients and to share information, subject to appropriate inter-agency agreements, on common clients.

In compliance with all state and federal requirements regarding client/consumer confidentiality and data security, the HMIS is designed to collect and deliver quality data about services and homeless persons or persons at risk for being homeless and meet the reporting requirements of the U.S. Department of Housing and Urban Development (HUD), and other funders as needed. DuPage County Community Services and The Alliance to End Homelessness of Suburban Cook County partner together to administer the HMIS for the DuPage County Continuum of Care.

II. HMIS LEAD Responsibilities

1. The HMIS LEAD will make a best effort to provide the AGENCY 24-hour access to the HMIS database system, except during routine system maintenance, scheduled system upgrades and unexpected system failures.
2. The HMIS LEAD will provide model Privacy Notices, Client forms and other templates for agreements that may be adopted or adapted in local implementation of HMIS functions.
3. The HMIS LEAD will provide both initial training and periodic updates for all end-users regarding the use of the HMIS.
4. The HMIS LEAD will provide basic user support and technical assistance (i.e., general troubleshooting and assistance with standard report generation).

III. AGENCY Responsibilities

1. The AGENCY agrees to abide by the most current *HMIS Standard Operating Procedure* (Policy) approved and adopted by the DuPage County Continuum of Care, which is incorporated into this agreement by reference and may be modified from time to time at the DuPage County Continuum of Care's discretion. The Policy includes privacy, security, and data entry requirements. If any item in this agreement differs from the Policy, the Policy shall prevail.
2. The AGENCY agrees to ensure that all employees and agents comply with the Policy.
3. The AGENCY agrees to ensure staffing and equipment necessary to implement and ensure HMIS participation.
4. The *HMIS Standard Operating Procedure* can be obtained online at dupagehomeless.org/HMIS/SOP.
5. The AGENCY agrees to designate an AGENCY DATA ADMINISTRATOR that will act as the agency's key point person in communicating with the HMIS LEAD. This person is to be designated in writing by the Chief Executive Officer, Executive Director or equivalent of the AGENCY.

IV. Privacy and Confidentiality

A. Protection of Client Privacy

1. The AGENCY will comply with all applicable federal and state laws regarding protection of client privacy.
2. The AGENCY will comply with all policies and procedures established by the HMIS LEAD pertaining to protection of client privacy.

B. Client Confidentiality

1. The AGENCY agrees to make available a copy of the A*GENCY'S Privacy Notice* (or an equivalent AGENCY-specific alternative) to each consumer. The AGENCY will provide a verbal explanation of the HMIS and arrange for a qualified interpreter/translator or other reasonable accommodation in the event that an individual is not literate in English or has difficulty understanding the A*GENCY'S Privacy Notice* and/or associated consent form(s).
2. The AGENCY will solicit or enter information about clients into the HMIS database only in order to provide services or conduct evaluation or research. AGENCY management, in consultation with the HMIS LEAD, will make a determination of what qualifies as essential for services or research.
3. The AGENCY will divulge any information received from the HMIS to any organization or individual only with proper written consent from the client, unless otherwise permitted by applicable regulations or laws, including exceptions outlined in AGENCY's Privacy Notice.
4. The AGENCY will ensure that all persons who are issued a User Identification and Password to the HMIS abide by this *HMIS Partner Agreement*, including all associated confidentiality provisions. The AGENCY will be responsible for oversight of its own related confidentiality requirements.
5. The AGENCY acknowledges that maintaining the confidentiality, security and privacy of information downloaded from the system by the AGENCY is strictly the responsibility of the AGENCY.

C. Inter-Agency Sharing of Information

1. The AGENCY acknowledges that all forms provided by the HMIS LEAD regarding client privacy and confidentiality are shared with the AGENCY as generally applicable models that may require specific modification in accord with AGENCY-specific rules. The AGENCY will review and revise (as necessary) all forms provided by the HMIS LEAD to assure that they are in compliance with the laws, rules and regulations that govern its organization.

2. The AGENCY acknowledges that client notification as defined by the Policy is required before any basic identifying client information is shared with other agencies in the System.

3. If the AGENCY intends to share restricted client data within the HMIS, the AGENCY will execute an HMIS data sharing agreement with each Agency with whom the restricted data is to be shared. Restricted information, including progress notes and psychotherapy notes, about the diagnosis, treatment, or referrals related to a mental health disorder, drug or alcohol disorder, HIV/AIDS, and domestic violence concerns shall not otherwise be shared with other participating Agencies. Agencies with whom restricted information is shared are each responsible for obtaining appropriate consent(s) before allowing further sharing of client records.

4. The AGENCY acknowledges that the AGENCY, itself, bears primary responsibility for oversight for all sharing of data it has collected via the HMIS. The HMIS LEAD will hold the AGENCY responsible only for information that the AGENCY shares. The HMIS LEAD, however, will not hold the AGENCY responsible for the actions of the Entity that receives and misappropriates the shared data; unless the AGENCY knew or should have known that the Entity would misappropriate or were otherwise not entitled to receive the shared information.

D. Custody of Data

If this Agreement is terminated, AGENCY will no longer have access to the HMIS. The HMIS LEAD shall make reasonable accommodations to assist the AGENCY to export their data in a format that is usable in their alternative database. Any costs associated with exporting the data will be the sole responsibility of the AGENCY.

V. Hold Harmless

1. The HMIS LEAD makes no warranties, expressed or implied. The AGENCY, at all times, will indemnify and hold the HMIS LEAD harmless from any damages, liabilities, claims, and expenses that may be claimed against the AGENCY; or for injuries or damages to the AGENCY or another party arising from participation in the HMIS; or arising from any acts, omissions, neglect, or fault of the AGENCY or its agents, employees, licensees, or clients; or arising from the AGENCY 's failure to comply with laws, statutes, ordinances, or regulations applicable to it or the conduct of its business. This AGENCY will also hold the HMIS LEAD harmless for loss or damage resulting in the loss of data due to delays, non-deliveries, deliveries in error, or service interruption caused by the HMIS software vendor, by the AGENCY's or other member agency's negligence or errors or omissions, as well as natural disasters or technological difficulties, and/or any other cause not under the reasonable control of the HMIS lead. The HMIS LEAD shall not be liable to the AGENCY for damages, losses, or injuries to the AGENCY or another party other than if such is the result of gross negligence or willful misconduct of the HMIS LEAD. The HMIS LEAD agrees to hold the AGENCY harmless from any damages, liabilities, claims or expenses caused solely by the negligence or misconduct of the HMIS LEAD.
2. Provisions of Section V shall survive any termination of the *HMIS Partner Agreement*. All restrictions on the use and disclosure of client information will also survive any termination of the *HMIS Partner Agreement*.

VI. Terms and Conditions

1. The parties hereto agree that this agreement is the complete and exclusive statement of the agreement between parties and supersedes all prior proposals and understandings, oral and written, relating to the subject matter of this agreement.
2. The Agency shall not transfer or assign any rights or obligations under the *HMIS Partner Agreement* without the written consent of the HMIS LEAD.
3. This agreement shall remain in force until revoked in writing by either party, with 30 days advance written notice. The exception to this term is if allegations or actual incidences arise regarding possible or actual breeches of this agreement. Should such situations arise, the HMIS LEAD may immediately suspend access to the HMIS until the allegations are resolved in order to protect the integrity of the system.
4. This agreement may be modified or amended by written agreement executed by both parties with 30 days advance written notice.

IN WITNESS WHEREOF, the parties have entered into this Agreement:

AGENCY:

Signature:

____

Printed Name:

____

Title:______________________

Date: ______________________

HMIS LEAD:

Signature:

____

Printed Name:

____

Title: ______________________

Date: ______________________

Homeless Management Information System

ASSURANCE

____ (Name of Agency) assures that the following fully executed documents will be on file and available for review.

□ The AGENCY’s official *Privacy Notice* for HMIS clients.

□ Executed End User Agreement for each AGENCY user of the HMIS.

□ Current copy of the *HMIS Standard Operating Procedure.*

By: ___________________________________

Title: __________________________________

Signature:______________________________

Date: __________________________________

HMIS Agency Data Administrator Policy and Code of Ethics

Agency Data Administrator Name (Please Print)

Responsibilities of each Agency Data Administrator

Each Participating Agency will have an Agency Data Administrator (ADA) designated in writing by the Chief Executive Officer, Executive Director, or equivalent.

The Agency Data Administrator will be responsible for the following:

(Initial each line below to indicate acknowledgement)

_______ Acting as the key point person in communicating with the HMIS Lead.

_______ Attending and participating in all required site visits and sharing information with necessary staff to ensure that the agency is effectively and properly utilizing the HMIS.

_______ Attending and participating in all ADA-specific training sessions to ensure ongoing understanding of the HMIS and its reporting capabilities, to stay informed about system updates, and to address common questions or concerns.

_______ Reviewing and coordinating with HMIS System Administrators to update agency information in the HMIS database.

_______ Notifying HMIS Staff of user changes as soon as possible, at minimum 24 hours after their occurrence. This includes staff departures as well as modifications in user roles.

_______ Training new staff persons on the uses of HMIS including review of the Standard Operating Procedures (SOP) and any agency policies that impact the security and integrity of client information.

_______ Ensuring that unsupervised access to the HMIS be granted to authorized staff members only after they completed all required training, demonstrated proficiency in use of the software and understanding of the SOP, and by passing the End User Exam.

_______ Communicate all relevant HMIS updates to agency staff members including but not limited to system downtime, software updates, data standard changes, common issues, etc.

_______ Generating reports for agency specific needs. This includes reviewing reports to ensure data integrity, data quality, and timeliness of data entry.

_______ Implementing an Agency data security policy and standards, including:

- Administering agency-specified business and data protection controls
- Administering and monitoring of access control
- Detecting and responding to violations of the SOPs or agency procedures
- Effectively communicating the Security Plan to individuals responsible for security at their agency

Acknowledgement

I acknowledge that I have read the responsibilities of the Agency Data Administrator and certify that I can perform these functions.

Agency: ____________________________________

Agency Data Administrator Signature:

____ Date: ______________________

HMIS End User Policy and Code of Ethics

HMIS User's First and Last Name

USER POLICY

Partner Agencies who use the Northeast Illinois Homeless Management Information System (HMIS) and each User within any Partner Agency is bound by various restrictions regarding Protected Personal Information ("PPI"). The employee, contractor, or volunteer whose name appears above is the User.

It is a client's decision about what level of information is to be shared with any Partner Agencies. If your agency is covered by HIPAA or 42 CFR Part 2 (federally defined treatment facility), it is also the Client's decision about whether this Agency or Northeast Illinois HMIS may use information for research purposes, unless certain other approvals have been obtained.

Before any PPI is designated for sharing, the User shall ensure that the agency's HMIS Notice of Privacy Practices was fully reviewed with Client in a manner to ensure that Client fully understood the information. Any PPI not covered in the HMIS Notice of Privacy Practices must be covered by a signed client consent prior to sharing.

USER PRINCIPLES

A User ID and Password gives you access to the Northeast Illinois HMIS. You must initial each item below to indicate your understanding and acceptance of the proper use of your ID and password. Failure to uphold the confidentiality standards set forth below is grounds for your immediate termination from the HMIS.

(Initial each line below)

________ I understand that I have an obligation to maintain Client privacy and to protect and safeguard the confidentiality of Client's PPI. PPI shall include, but not be limited to, the Client's name, address, telephone number, social security number, type of medical care provided, medical condition or diagnosis, veteran status, employment information, and all other information relating to the Client's programming.

________ My User ID and Password are for my use only and must not be shared with anyone, including my supervisor(s). I must take all reasonable means to keep my Password physically secure.

________ I understand that the only individuals who can view information in the HMIS are authorized users who need the information for legitimate business purposes of this Agency and the Clients to whom the information pertains.

________ I may only view, obtain, disclose, or use information within the HMIS that is necessary to perform my job.

________ If I am logged into the HMIS and must leave the work area where the computer is located, I must logoff before leaving the work area.

________ Any hard copies of PPI printed from the HMIS must be kept in a secure file, and destroyed when no longer needed, in accordance with Agency's records retention policy. I will not leave hard copies of PPI in public view on my desk, or on a photocopier, printer, or fax machine.

________ I will not discuss PPI with anyone in a public area.

________ I have reviewed the Agency's Privacy Notice and the *HMIS Standard Operating Procedures*, understand each of those documents, and agree to abide by them.

________ If I notice or suspect a security breach, I must immediately notify the Agency Data Administrator or in their absence the Executive Director. The Agency Data Administrator and Executive Director are responsible for acting as instructed in the Standard Operating Procedures.

_______ I understand that any violation of this Agreement can lead to the suspension of my system access, and notification of such will be sent to my Employer.

USER CODE OF ETHICS

A. Users must be prepared to answer Client questions regarding the HMIS.
B. Users must respect Client preferences with regard to the sharing of PPI within the HMIS. Users must accurately record Client's preferences by making the proper designations as to sharing of PPI and/or any restrictions on the sharing of PPI.
C. Users must allow Client to change his or her information sharing preferences at the Client's request (i.e., to revoke consent) (except if that policy is over-ridden by Agency policy or if the information is required to be shared as a condition of a provider agreement).
D. Users must not decline services to a Client or potential Client if that person refuses to share his or her personal information with other service providers via the HMIS (except if that policy is over-ridden by Agency policy or if the information is required to be shared as a condition of a provider agreement).
E. The User has primary responsibility for information entered by the User. Information Users enter must be truthful, accurate and complete to the best of User's knowledge.
F. Users will follow the Standard Workflow, answering all Universal and Program Specific Data Elements as described by local and Federal HMIS policies.
G. Users will not solicit from or enter information about Clients into the HMIS unless the information is required for a legitimate business purpose such as to provide services to the Client.
H. Users will not include profanity or offensive language in the HMIS; nor will Users use the HMIS database for any violation of any law, to defraud any entity or conduct any illegal activity.

PASSWORD PROCEDURES

By signing this Agreement, you agree that passwords

A. Are your responsibility and may not be shared.
B. Should be securely stored and inaccessible to other persons—including your supervisor(s).
C. Should never be stored or displayed in any publicly accessible location.
D. Should not be transmitted electronically.

USER GRIEVANCE PROCEDURE

If you have a grievance with this Code of Ethics, you may send a written complaint to your Employer. If your complaint is not resolved to your satisfaction, you may send your written complaint to: DuPage County HMIS, 421 N County Farm Road, Wheaton, IL 60187, Attn: HMIS Manager.

I understand and agree to comply with the above User Policy, User Principles, User Code of Ethics, Password Procedures, and User Grievance Procedure.

HMIS User Signature: ______________________________________ Date:_____________________

Username: ____

Email Address: ____

Agency/System Administrator: ________________________________ Date: ________________________

Section 2: Privacy Plan

Privacy Plan Overview

On July 30, 2004, the US Department of Housing and Urban Development (HUD) released the standards for Homeless Management Information Systems (69 Federal Register 45888). This standard outlines the responsibilities of the HMIS and for the agencies which participate in an HMIS. This section of our Standard Operating Procedure describes the Privacy Plan of the DuPage County HMIS. We intend our policy and plan to be consistent with the HUD standards. All users, agencies and system administrators must adhere to this Privacy Plan.

We intend our Privacy Plan to support our mission of providing an effective and usable case management tool. We recognize that clients served by individual agencies are not exclusively that “agency’s client” but instead are truly a client of the DuPage County Continuum of Care. Thus, we have adopted a Privacy Plan which supports limited sharing of client-level data with the intent to improve coordination of care and resource linkages amongst partnering agencies.

The core tenant of our Privacy Plan is the Baseline Privacy Notice. The Baseline Privacy Notice describes how client information may be used and disclosed and how clients can get access to their information. Each agency must either adopt the Baseline Privacy Notice or develop a Privacy Notice which meets or exceeds all minimum requirements set forth in the Baseline Privacy Notice (this is described in the Agency Responsibilities section of this Privacy Plan). This ensures that all agencies who participate in the HMIS are governed by the same minimum standards of client privacy protection. Although the Baseline Privacy Notice and its related forms are appendices to this section, they act as the cornerstone of our Privacy Plan.

All amendments to the Privacy Plan (including changes to the Baseline Privacy Notice and related forms) are proposed by the Data & Performance Committee and reviewed by the Leadership Committee of the DuPage County Continuum of Care. All forms as referenced are posted online, dupagehomeless.org/hmis/forms.

Privacy Plan Documents & Forms	Description	Use by Agency
Baseline Privacy Notice	This is the main document of this Privacy Plan. This document outlines the minimum standard by which an agency collects, utilizes and discloses information.	*REQUIRED* Agencies must adopt a privacy notice which meets all minimum standards.
Privacy Posting	This posting explains the reason for asking for personal information and notifies the client of the Privacy Notice.	*REQUIRED* Agencies must adopt and utilize a Privacy Posting.
Request to Not Share Information in HMIS	This form gives the client the opportunity to opt out or revoke the sharing of their information to other agencies in HMIS.	*REQUIRED* Agencies must have this form available for the client.
Acknowledgement of Receipt	This form provides physical documentation that the client was informed of the privacy notice and their rights regarding opting-out of data sharing.	*Optional* Agencies are encouraged, but not required to utilize this form.

User Responsibilities

A client's privacy is upheld only to the extent that the users and direct service providers protect and maintain their privacy. The role and responsibilities of the user cannot be over-emphasized. A user is defined as a person that has direct interaction with a client or their data. (This could potentially be any person at the agency: a staff member, volunteer, contractor, etc.)

Users have the responsibility to:

- Understand their agency's Privacy Notice.
- Be able to explain their agency's Privacy Notice to clients.
- Follow their agency's Privacy Notice.
- Know where to refer the client if they cannot answer the client's questions.
- Present their agency's Privacy Notice to the client before collecting any information.
- Uphold the client's privacy in the HMIS.

Agency Responsibilities

The 2004 HUD HMIS Standards emphasize that it is the agency's responsibility for upholding client privacy. All agencies must take this task seriously and take time to understand the legal, ethical and regulatory responsibilities. This Privacy Plan and the Baseline Privacy Notice provide guidance on the minimum standards by which agencies must operate if they wish to participate in the HMIS.

Meeting the minimum standards in this Privacy Plan and the Baseline Privacy Notice are required for participation in the HMIS. Any agency may exceed the minimum standards described and are encouraged to do so. Agencies must have an adopted Privacy Notice which meets the minimum standards before data entry into the HMIS can occur.

Agencies have the responsibility to:

- Review their program requirements to determine what industry privacy standards must be met that exceed the minimum standards outlined in this Privacy Plan and Baseline Privacy Notice (examples: Substance Abuse Providers covered by 24 CFR Part 2, HIPAA Covered Agencies, Legal Service Providers).
- Review the 2004 HUD HMIS Privacy Standards (69 Federal Register 45888)
- Adopt and uphold a Privacy Notice which meets or exceeds all minimum standards in the Baseline Privacy Notice as well as all industry privacy standards. The adoption process is to be directed by the individual agency. Modifications to the Baseline Privacy Notice must be approved by the HMIS Committee.
- Ensure that all clients are aware of the adopted Privacy Notice and have access to it. If the agency has a website, the agency must publish the Privacy Notice on their website.
- Make reasonable accommodations for persons with disabilities, language barriers or education barriers.
- Ensure that anyone working with clients covered by the Privacy Notice can meet the User Responsibilities.
- Designate at least one user that has been trained to technologically uphold the agency's adopted Privacy Notice.

System Administration Responsibilities

DuPage County Community Services HMIS Staff have the responsibility to:

- Adopt and uphold a Privacy Notice which meets or exceeds all minimum standards in the Baseline Privacy Notice.
- Train and monitor all users with System Administrator access on upholding system privacy.
- Monitor agencies to ensure adherence to their adopted Privacy Notice.
- Develop action and compliance plans for agencies that do not have adequate Privacy Notices.
- Maintain the HMIS Website to keep all references within the Baseline Privacy Notice up to date.
- Provide training to agencies and users on this Privacy Plan.

[Agency Logo Here]

HMIS Notice of Privacy Practices

Effective **[SELECT A DATE]**

THIS NOTICE DESCRIBES HOW INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN ACCESS THIS INFORMATION.

[Agency Name] and the Northeast Illinois Homeless Management Information System (HMIS)

Overview

When you request services from [Agency Name], information about you and members of your family is entered into a computer system called HMIS, or Homeless Management Information System. HMIS is a project of DuPage County Community Services in partnership with many organizations in northeast Illinois that provide homeless, health care, medical, and social services to persons and families in need. The information collected in HMIS will help us coordinate and provide better service, document the need for additional services, and generate reports such as the number of persons who are homeless or at risk of homelessness in northeast Illinois.

We intend our policy and practices to align with the Housing and Urban Development's (HUD) HMIS Data and Technical Standards and HMIS Data Standards[1].

What is Being Shared

This agency's staff and the Software Administrators have access to all data collected in HMIS, and the participating agencies have limited access as described below and online, dupagehomeless.org/HMIS/Forms. If further information is to be shared and is not covered by this notice, then a separate authorization will be required.

Information shared to participating agencies include:

- Protected Personal information (PPI) - Name, Date of Birth, and Social Security Number. PPI is information that allows identification of an individual directly or indirectly, can be manipulated by a reasonably foreseeable method to identify a specific individual, or can be linked with other available information to identify a specific client.
- Demographics – Race, Ethnicity, Gender, Veteran Status
- Project Enrollments – Project Name, Enrollment dates, Reason for Leaving a program, and the Housing Destination you left to.
- Case Manager's contact information (if one is assigned)

How Your Information May Be Used

Unless restricted by law, the information can be used by:

- Authorized people who work in [Agency Name], HMIS partner organizations for administrative purposes related to providing and coordinating services to you or your family, or for billing or funding purposes.
- Auditors or others who review the work of [Agency Name] or need to review the information to

[1] https://www.hudexchange.info/programs/hmis/

provide services to [Agency Name].

- The HMIS system administrator(s), DuPage County Community Services and its designees, and the HMIS developer (WellSky) for administrative purposes (for example, to assist [Agency Name] by checking for data errors and identifying your potential eligibility for services).
- Individuals performing academic research who have signed a research agreement with [Agency Name] or DuPage County Community Services. Your name, social security number or other identifying information may be used to match records but will not be used directly in the research unless you sign a separate consent.
- [Agency Name] or the DuPage County Community Services may use your information to create aggregate data that has your identifying information removed. Also, [Agency Name] may disclose to a third-party aggregate data so that the third party can create data that does not include any of your identifying information.
- Government or social services agencies that are authorized to receive reports of homelessness, abuse, neglect, or domestic violence, when such reports are required by law or standards of ethical conduct.
- A coroner or medical examiner or funeral director to carry out their duties.
- Authorized federal officials for the conduct of certain national security or certain activities associated with the protection of certain officials.
- Law enforcement officials, but the disclosure must meet the minimum standards necessary for the immediate purpose and not disclose information about other individuals. A court order or search warrant may be required.
- Others, to the extent that the law requires a specific use or disclosure of information. Information may be released to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; if the disclosure is made to a person or persons reasonably able to prevent or lessen the threat or harm, including the target of a threat.

Other uses and sharing of your information will be made *only with your written consent*.

Your Rights Regarding Your Information in HMIS

- You have the right to opt-out of having your and your household members' information shared to partnering agencies in the Northeast Illinois Homeless Management Information System (HMIS). To do so, you must request and sign the "Request to Not Share Information in HMIS." Any information in the HMIS prior to signing the form will continue to be shared with the agencies as described in this notice.
- You may request a list of current HMIS partner organizations from [Agency Name], DuPage County Community Services, or review the current list at suburbancook.org/hmis. Northeast Illinois HMIS may add new HMIS partner organizations to this list at any time.
- You have the right to inspect and obtain a copy of your own protected personal information for as long as it is kept in the HMIS, except for information compiled in reasonable anticipation of, or for use in, a legal proceeding.

- You have the right to request a correction of your protected personal information when the information in the record is inaccurate or incomplete.

Enforcement of Your Rights

If you believe your privacy rights have been violated, you may send a written complaint to [Agency Name]. If your complaint is not resolved to your satisfaction, you may send your written complaint to DuPage County Community Services. Addresses are listed at the end of this Notice. You will not be retaliated against for filing a complaint.

[Agency Name] is required by law to maintain the privacy of your protected personal information, and to display a copy of the most recent Notice. [Agency Name] reserves the right to change the Notice from time to time, and if it does, the change will affect all the information in the HMIS, not just the information entered after the change. The revised Notice will be posted at [Agency Website]. You may request a copy of it from [Agency Name].

[Agency Contact Information]
[Address]
[Address]
[Phone Number]
[Website]

DuPage County Community Services
HMIS System Administrator
421 N County Farm Road
Wheaton, IL 60187
630-407-6397
dupagehomeless.org/HMIS

Change History

- October 2009- Initial Policy was a part of client consent documents.
- October 2012 - Adopted HUD's baseline privacy notice and detailed our implied consent disclosure process.
- October 2014 – Updated HUD's baseline privacy notice to include Suburban Cook County, address the name change of DuPage County HMIS to Northeast Illinois HMIS, and reflect the changes to the list of shared data elements.
- June 2021 – Complete reorganization, re-formatting, deduplication of statements, and adjusted level of language used. Added language around sharing of pre-existing data after a client refuses to share any new information. Moved to using Effective date rather than version numbers.
- April 2022 – Updated websites.
- January 2024 – Updated name of the form used to opt out of sharing information in HMIS. Added the name of the regional HMIS implementation, Northeast Illinois.

DuPage County CoC
HMIS Data Sharing Summary

An updated list of Northeast Illinois Homeless Management Information System (HMIS) participating agencies are available at, suburbancook.org/hmis.

Information Shared to all Participating Agencies

- Full Name & Alias
- Date of Birth
- Social Security Number
- Gender
- Race
- Ethnicity
- Household Relationships
- Veteran Status
- Photograph
- Primary Language Spoken
- Case Manager
- Name of Program Enrolled In
- Program Enrollment Dates
- Reason for Leaving the Program
- Housing Destination After leaving the Program

[Agency Logo Here]

DUPAGECOUNTY CONTINUUM OF CARE
Working to end homelessness

Acknowledgement of Receipt

Notice of [Agency's] Privacy Notice

[This Agency] is required to maintain a Privacy Notice. The Privacy Notice describes the information we collect, how we manage that information and your rights and choices pertaining to that information.

[This Agency] participates in a Homeless Management Information System (HMIS) along with many other agencies. Unless you request and sign the "Data Sharing Refusal Form," much of your information will be shared with these other agencies for the purposes disclosed in the Privacy Notice. The information shared is discussed in the Privacy Notice.

If you would like a copy of the Privacy Notice or would like to request that your information is not shared in HMIS, please ask.

Declining to sign this acknowledgement does not prevent us from using or disclosing your information. To prevent disclosure of your information in HMIS, you must complete the "Request to Not Share Information in HMIS" form. Your decision to not sign this acknowledgement will be documented along with the fact that you were informed of our Privacy Notice.

I have reviewed the above information and I confirm that:

- I was offered a copy of [This Agency's] Privacy Notice.
- I have reviewed [This Agency's] Privacy Notice. I was given the option to have this document and the Privacy Notice read to me.
- I had the opportunity to ask questions about [This Agency's] Privacy Notice and about how information about me and my family will be shared with other agencies who participate in the HMIS.
- I was advised of my rights including my rights to not share my information in HMIS.
- I understand that services cannot be denied to me if I choose not to share my information in HMIS.

Name of Client or Guardian: ___________________________________

Signature of Client or Guardian: ________________________________ Date: _____________

[Agency Logo Here]

Request to Not Share Information in HMIS

I hereby opt-out and/or revoke permission for [Agency Name] to share my personal and household information with other agencies in the Northeast Illinois Homeless Management Information System (HMIS). I understand that by not sharing my information with other agencies, I may be limiting my options for service coordination. I also understand that any information entered in HMIS prior to submission of this form will continue to be shared as described in the Privacy Notice.

However, all information that I provide will remain in the HMIS for the purposes disclosed in the Privacy Notice. This information will be accessible to the HMIS System Administrators and disclosure may still occur in accordance with the Privacy Notice. The Privacy Notice is available to me upon request.

Members of this household whose information will also not be shared:

Name	HMIS Number

______________________________ ______________________________ ______________

Name of Client or Guardian Signature of Client or Guardian Date

To be filled out by Agency:

___ I certify that I followed the necessary steps to ensure the client's HMIS profile was set up correctly.

OR

___ I contacted the DuPage County HMIS Help Desk to request set up of the client's HMIS profile.

____________________________ _____________________________ ______________

Staff Name Signature Date

Section 3: Data Quality Plan

Introduction to Data Quality

Data quality in the Homeless Management Information System (HMIS) is crucial for accurately representing the reality of homelessness and program and system performance. To achieve good data quality, data must be assessed using a client centered approach, all tools must align with HMIS Data Standards and our local Data Quality Plan, and all data entry is to be completed in a timely fashion using a HMIS Staff approved workflow.

The Data Quality Plan applies to all HMIS partners regardless of project type or funding source as described in the table below. HMIS Users should regularly review the HMIS Data Standards Manual and related program manuals [1] for further guidance. Victim Service Providers (VSP) shall maintain a comparable database that meets all minimum Federal and local data collection and reporting requirements, where all project data for any VSP will be maintained in the CoC HMIS.

Data Coverage

The concept of data coverage refers to the sample size and diversity of the agencies and programs who utilize the HMIS. If we want an accurate picture of our community, we must not overlook any agency or program providing services within the Continuum of Care. It is important to note that this includes HUD funded and non-HUD funded programs and agencies.

Bed Coverage Rate

DuPage Continuum of Care has set a threshold of 100% bed coverage rates for dedicated homeless lodging providers in HMIS. VSP point-in-time data will be submitted to HMIS annually, or more frequently as needed, from their HMIS comparable database.

The Bed Coverage Rate is calculated by project type,

= (# dedicated homeless beds in HMIS) *divided by* (# dedicated homeless beds in DuPage CoC)

Other

The Data & Performance Committee, along with the partnership of DuPage Continuum of Care's Leadership and related committees, will continue to assess community data needs, including the inclusion of new agencies and data elements.

Data Quality

Data Quality is broken down into 5 equally important components: Completeness, Timeliness, Accuracy, Training and Consistency. Each of these components must be individually monitored by those completing the data entry, Agency Data Administrators, and System Administrators.

Completeness

HMIS and Agency Data Administrators are to ensure that the Project Descriptor Data Elements are

[1] https://www.hudexchange.info/programs/hmis/hmis-guides/#project-setup-and-data-collection-resources

complete for all HMIS projects[2] and that the data is reviewed annually for each project.

Each participating agency, project, Agency Data Administrator, and user entering data into HMIS must ensure that Client Records have complete data elements that accurately reflect the client situation at that point in time, achieving an Error Rate[3] less than the amount as specified in the Data Quality Error Rate Thresholds Table below.

Data Quality Error Rate Thresholds

Element Type	Data Element	For Whom	Collection Point	Project Type	Error Rate Threshold	Tools to Measure
Project Descriptor	Organization Information	All Projects	Creation and reviewed annually	All Projects	0%	– 0227 Project Descriptor Elements Data Quality
Project Descriptor	Project Information	All HMIS Projects	Creation and reviewed annually	All HMIS Projects	0%	– 0227 Project Descriptor Elements Data Quality – Housing Inventory Count
Project Descriptor	Continuum of Care Information	All HMIS Projects	Creation and reviewed annually	All HMIS Projects	0%	– 0227 Project Descriptor Elements Data Quality – Housing Inventory Count
Project Descriptor	Funding Sources	All HMIS Projects	Creation and reviewed annually	All HMIS Projects	0%	– 0227 Project Descriptor Elements Data Quality – Housing Inventory Count
Project Descriptor	Bed and Unit Information	All HMIS Projects	Creation and re-assessed quarterly	ES, SH, TH, RRH, PSH, and all PH.	0%	– 0227 Project Descriptor Elements Data Quality – Housing Inventory Count
Project Descriptor	HMIS Participation Status	All HMIS Projects	Creation and	All HMIS Projects	0%	– TBD

[2] HMIS Projects are projects that are dedicated to ending or preventing homelessness such as Street Outreach (SO), Emergency Shelter (SO), Transitional Housing (TH), Safe Haven (SH), all Permanent Housing (PH - RRH, PSH, Other), Supportive Services only (SSO), and Coordinated Entry (CE).

[3] Error Rate includes null, client doesn't know, client refused/client prefers not to answer, data not assessed, and incongruent data.

Section 3: Data Quality Plan

Element Type	Data Element	For Whom	Collection Point	Project Type	Error Rate Threshold	Tools to Measure
			reviewed annually			
Project Descriptor	CE Participation Status	All HMIS Projects	Creation and reviewed annually	All HMIS Projects	0%	– TBD
Universal Data Element	Name and Name Data Quality	All Clients	Record Creation	All HMIS Projects	5%	– Data Quality Framework – APR – ESG CAPER
Universal Data Element	[4]Full or last 4 of the Social Security Number (SSN) and SSN Data Quality	All Clients	Record Creation	All HMIS Projects	10%	– Data Quality Framework – APR – ESG CAPER
Universal Data Element	Date of Birth and Date of Birth Data Quality	All Clients	Record Creation	All HMIS Projects	5%	– Data Quality Framework – APR – ESG CAPER
Universal Data Element	Race and Ethnicity	All Clients	Record Creation	All HMIS Projects	5%	– Data Quality Framework – APR – ESG CAPER
Universal Data Element	Gender	All Clients	Record Creation	All HMIS Projects	5%	– Data Quality Framework – APR – ESG CAPER
Universal Data Element	Veteran Status	All Adults	Record Creation	All HMIS Projects	10%	– Data Quality Framework – APR – ESG CAPER
Universal Project Stay Element	Disabling Condition (Y/N)	All Clients	Project Start	All HMIS Projects	10%	– Data Quality Framework – APR – ESG CAPER
Universal Project Stay Element	Project Start Date	All Clients	Project Start	All HMIS Projects	10%	– Data Quality Framework – APR – ESG CAPER
Universal Project Stay Element	Destination at Exit	All Clients	Project Exit	Emergency Shelter (ES) and Street Outreach (SO)	21%	– Data Quality Framework – APR – ESG CAPER
				All Other HMIS Projects	10%	

[4] Agencies should check with their funder to determine if the full vs. last 4 of the SSN is a requirement for their program.

Section 3: Data Quality Plan

Element Type	Data Element	For Whom	Collection Point	Project Type	Error Rate Threshold	Tools to Measure
Universal Project Stay Element	Relationship to Head of Household	All Clients	Project Start	All HMIS Projects	5%	– Data Quality Framework – APR – ESG CAPER
Universal Project Stay Element	Client Location	Head of Household	Project Start, Update	All HMIS Projects	5%	– Data Quality Framework – APR – ESG CAPER
Universal Project Stay Element	Prior Living Situation and related fields	Head of Household, Adults	Project Start	All HMIS Projects	10%	– Data Quality Framework – APR – ESG CAPER
Program Specific Data Element	Income	Head of Household, Adults	Project Start, Update, Exit	All HMIS Projects	10%	– Data Quality Framework – APR – ESG CAPER
Program Specific Data Element	Income	Head of Household, Adults	Annual	ES	49%	– Data Quality Framework – APR – ESG CAPER
				SO	90%	
				All Other HMIS Projects	20%	
Program Specific	Non-Cash Benefits	Head of Household, Adults	Project Start, Update, Annual, Exit	ES	49%	– Data Quality Framework – APR – ESG CAPER
				SO	90%	
				All HMIS Projects	10%	
Program Specific	Health Insurance	All Clients	Annual	ES	49%	– APR – ESG CAPER
				SO	90%	
				All Other HMIS Projects	20%	
Program Specific	Disability	All Clients	Project Start, Update, Exit	All HMIS Projects	10%	– APR – ESG CAPER
Program Specific	Domestic Violence	Head of Household, Adults	Project Start, Update	All HMIS Projects	10%	– APR – ESG CAPER
Program Specific	Current Living Situation	Head of Household, Adults	At occurrence	Coordinated Entry (CE) and SO	10%	– ESG CAPER
Program Specific	Engagement	Head of Household, Adults	At occurrence	SO	NA	– ESG CAPER
Program Specific	Coordinated Entry Assessment	Head of Household	At Occurrence	Coordinated Entry	NA	– TBD

Section 3: Data Quality Plan

Element Type	Data Element	For Whom	Collection Point	Project Type	Error Rate Threshold	Tools to Measure
Program Specific	Coordinated Entry Event	Head of Household	At Occurrence	Coordinated Entry	NA	– TBD
Federal Partner Program Specific	Percent of AMI	Head of Household, Adults	Project Start, Update, Annual, Exit	All HMIS Projects	10%	– Basic Demographic and EE Details – SSVF Export (for SSVF projects only)
Federal Partner Program Specific	Moving On Assistance	Head of Household	At occurrence	PSH	NA	– TBD
Federal Partner Program Specific	Translation Assistance Needed	Head of Household	Project Start	All HMIS Projects	NA	– TBD
Federal Partner Program Specific	Housing Assessment at Exit	All Clients	Project Exit	HP	NA	– TBD
Federal Partner Program Specific	Connection with SOAR	Head of Household and Adults	Project Start, Update, Annual, and Exit	SSVF HP and RRH	NA	– TBD
Federal Partner Program Specific	Referral Source	Head of Household and Adults	Project Start	All RHY	NA	– 0263 RHY Data Completeness – Hashed HMIS CSV and RHYMIS
Federal Partner Program Specific	Sexual Orientation	Head of Households and Adults	Project Start	PSH and All RHY	NA	– 0263 RHY Data Completeness – Hashed HMIS CSV and RHYMIS
Federal Partner Program Specific	Last Grade Completed	Head of Household and Adults	Project Start and Exit	All VASH, SSVF, and RHY	NA	– 0263 RHY Data Completeness – Hashed HMIS CSV and RHYMIS
Federal Partner Program Specific	School Status	Head of Household and Adults	Project Start and Exit	All RHY	NA	– 0263 RHY Data Completeness – Hashed HMIS CSV and RHYMIS
Federal Partner Program Specific	Employment Status	Head of Household and Adults	Project Start and Exit	All VASH, SSVF, GPD	NA	– 0263 RHY Data Completeness – Hashed HMIS CSV and RHYMIS

Section 3: Data Quality Plan

Element Type	Data Element	For Whom	Collection Point	Project Type	Error Rate Threshold	Tools to Measure
Federal Partner Program Specific	General Health	Head of Household and Adults	Project Start and Exit	All VASH and RHY	NA	– 0263 RHY Data Completeness – Hashed HMIS CSV and RHYMIS
Federal Partner Program Specific	Dental Health	Head of Household and Adults	Project Start and Exit	All RHY	NA	– 0263 RHY Data Completeness – Hashed HMIS CSV and RHYMIS
Federal Partner Program Specific	Mental Health Status	Head of Household and Adults	Project Start and Exit	All RHY	NA	– 0263 RHY Data Completeness – Hashed HMIS CSV and RHYMIS
Federal Partner Program Specific	Pregnancy Status	Head of Household and Adults	Project Start and Exit	All RHY	NA	– 0263 RHY Data Completeness – Hashed HMIS CSV and RHYMIS
Federal Partner Program Specific	Formerly a Ward of Child Welfare/Foster Care Agency	Head of Household and Adults	Project Start	All RHY	NA	– 0263 RHY Data Completeness – Hashed HMIS CSV and RHYMIS
Federal Partner Program Specific	Formerly a Ward of Juvenile Justice System	Head of Household and Adults	Project Start	All RHY	NA	– 0263 RHY Data Completeness – Hashed HMIS CSV and RHYMIS
Federal Partner Program Specific	Family Critical Issues	Head of Household and Adults	Project Start	All RHY	NA	– 0263 RHY Data Completeness – Hashed HMIS CSV and RHYMIS
Federal Partner Program Specific	RHY Service Connections	Head of Household and Adults	At Occurrence	All RHY	NA	– 0263 RHY Data Completeness – Hashed HMIS CSV and RHYMIS
Federal Partner Program Specific	Commercial Sexual Exploitation/Sex Trafficking	Head of Household and Adults	Project Exit	All RHY	NA	– 0263 RHY Data Completeness – Hashed HMIS CSV and RHYMIS
Federal Partner Program Specific	Labor Exploitation/Trafficking	Head of Household and Adults	Project Exit	All RHY	NA	– 0263 RHY Data Completeness – Hashed HMIS CSV and RHYMIS

Section 3: Data Quality Plan

Element Type	Data Element	For Whom	Collection Point	Project Type	Error Rate Threshold	Tools to Measure
Federal Partner Program Specific	Project Completion Status	Head of Household and Adults	Project Exit	All RHY	NA	– 0263 RHY Data Completeness – Hashed HMIS CSV and RHYMIS
Federal Partner Program Specific	Counseling	Head of Household and Adults	Project Exit	All RHY	NA	– 0263 RHY Data Completeness – Hashed HMIS CSV and RHYMIS
Federal Partner Program Specific	Safe and Appropriate Exit	Head of Household and Adults	Project Exit	All RHY	NA	– 0263 RHY Data Completeness – Hashed HMIS CSV and RHYMIS
Federal Partner Program Specific	Aftercare Plans	Head of Household and Adults	Project Exit	All RHY	NA	– 0263 RHY Data Completeness – Hashed HMIS CSV and RHYMIS
Federal Partner Program Specific	Veteran's Information	All Veterans	Project Start	All VA and VASH	NA	– SSVF Data Quality
Federal Partner Program Specific	Services Provided - SSVF	All clients receiving services	At Occurrence	All SSVF	NA	– SSVF Data Quality
Federal Partner Program Specific	Financial Assistance – SSVF	All clients receiving financial assistance	At Occurrence	All SSVF	NA	– SSVF Data Quality
Federal Partner Program Specific	VAMC Station Number	Head of Household	Project Start	All VA and VASH	NA	– SSVF Data Quality
Federal Partner Program Specific	HP Targeting Criteria	Head of Household	Project Start	SSVF HP	NA	– SSVF Data Quality
Federal Partner Program Specific	HUD VASH Voucher Tracking	Head of Household/Veteran	At Occurrence	VASH	NA	– TBD
Federal Partner Program Specific	HUD VASH Exit Information	Head of Household/Veteran	Project Exit	VASH	NA	– TBD

Section 3: Data Quality Plan

Timeliness

To ensure accuracy of our data at any given time, HMIS data entry is to be completed in less than 7 days of the client interaction. Timeliness standards apply to all projects and information collected and entered into HMIS, including but not limited to assessment data, project entries, annual reviews, project exits, and service transactions.

Our committee has determined timeliness thresholds for Entry and Annual reviews, as shown in the Timeliness Thresholds table below, with the goal of continued improvement over time. No project can retroactively improve this measure but can establish protocols to help ensure timely data entry going forward. Given our HMIS's capabilities, we have determined that we are unable to provide an accurate measure of timeliness at Exit. We will continue to work with our Vendor to address this matter and will utilize quarterly point-in-time reporting and project specific reports to help ensure timely project exits.

Timeliness Thresholds

Timeliness Measure	Description	Project Type	Threshold: 7+ Days	Tools to Measure
Program Start	A Program Start Date will be created less than 7 days from the first day of service (ES, TH, SSO), contact (SO), or eligibility determination (all PH). The Program Start Date will be equal to the first day of service (ES, TH, SSO), contact (SO), or eligibility determination (PH).	All HMIS Projects	25%	– Data Quality Framework – APR – ESG CAPER – Point-in Time/Housing Inventory Supplemental
Annual Review	Required for all clients in a project for 365 days or more. Annual Reviews must be completed within 30 days from the anniversary of the Head of Household's project start date.	All HMIS Projects	25%	– Data Quality Framework – APR – ESG CAPER – Annual Review Dashboard Report
Program Exit	A Program Exit Date will be recorded in HMIS in less than 7 days of learning of the client's last service date or residence date. The Exit Date will be equal to the last day of service or residence.	All HMIS Projects, but SO and CE	Not Available	NONE – Our system does not capture the date an Exit record is created, but rather when the Entry/Exit record is updated. This is not an accurate reflection of when an Exit is created, therefore we are unable to accurately measure the timeliness of this data element. We recommend agencies utilize current reporting to spot check for accurate service and bed utilization. Those reports include: – Data Quality Framework – APR – ESG CAPER – Point-in Time

Timeliness Measure	Description	Project Type	Threshold: 7+ Days	Tools to Measure
Program Exit	A Program Exit Date will be recorded in HMIS in less than 7 days of learning of the client leaving the program, or when it has been 30 days since the last Contact (tracked in Current Living Situation). The Exit Date will be equal to the last day a Contact was made.	SO, CE	Not Available	NONE – Our system does not capture the date an Exit record is created, but rather when the Entry/Exit record is updated. This is not an accurate reflection of when an Exit is created, therefore we are unable to accurately measure the timeliness of this data element. We recommend agencies utilize current reporting to spot check for accurate service and bed utilization. Those reports include: – ESG CAPER – Trifecta – Point-in Time – By Name List

Accuracy

When collecting personal information, a client-centered approach should be used. Every client must be asked for their self-reported information. Staff observations should never be used to collect information regarding how a client identifies. Inaccurate data, whether intentional or unintentional, is generally worse than incomplete information as it allows for acknowledging gaps. Thus, it should be emphasized to clients and staff that it is better to enter nothing than to enter inaccurate information.

Agencies are required to monitor their own accuracy using some of the following guidelines:

- If using paper assessments, ensure that all required data elements are included, matching all client options and wording. DuPage has a Universal Intake form available online, dupagehomeless.org/hmis/forms.
- Review data quality and program specific reports for inaccurate information (a negative age, single child enrollment, minor who is a veteran, etc.)
- Confirm that the client understands what is being asked of them, they know what their options are, and that staff do not stray from the intent of the question.
- Audit a random sample of client records.
- Thoroughly review information with the client at program start, update, annual, and exit, ensuring the information provided is current and complete.
- Verify that the project start, annual review, and exit dates are accurate and complete for all participants. (See Timeliness Threshold Table).

Section 3: Data Quality Plan

Training

End User training is a major component to a data quality plan. The roles and responsibilities of training users is outlined in the following: Section 1 of this SOP, DuPage Continuum of Care and HMIS Memorandum of Understanding, HMIS Partnership Agreement, Agency Data Administrator Agreement, and the End User Agreement.

All users must complete new user training prior to receiving access to the HMIS. Training may be provided through the System or Agency Data Administrator. New user training must review the Standard Operating Procedures, HMIS software, and the data entry workflow, in addition to any project specific information. Users will be expected to demonstrate understanding and proper data entry workflow prior to obtaining access to the live site. Alternative training modules may be required depending on the user's role and access in the system.

To stay current and maintain access to HMIS, all Users must complete an annual training provided by System Administrators. Training topics will include privacy, security, data standards, and common issues and questions.

Agency Data Administrators or an agency/program representative shall participate in Agency Data Administrator trainings, and in turn relay this and all HMIS related information to the agency users.

If, at any time, a user is not able to demonstrate proper use or knowledge of the system or has not completed the required training, they will lose access to the system.

Consistency

The ability to accurately generate system-level reports is dependent upon a common understanding of the data being captured, options being provided to the client, ensuring only the client responses are being entered, and all tools meeting minimum data collection requirements where data is not directly captured in HMIS. It is up to each agency to ensure adherence to HMIS Staff approved data entry workflows.

Monitoring Data Quality

Monitoring Data Quality is a shared responsibility between the participating agency, HMIS Staff and the Data & Performance Committee. Each of the 5 elements of data quality (Completeness, Timeliness, Accuracy, Training and Consistency) is to be monitored.

Agency and Program data quality is to be monitored by the Agency Data Administrator monthly. Each agency may choose different reports to monitor their data quality. Each Agency Data Administrator should work with the HMIS Staff to ensure they are running correct data quality reports. HMIS Staff may set up a schedule by which agencies are required to submit specific data quality reports to the HMIS Lead for review.

Section 3: Data Quality Plan

As a guideline, the HUD CoC APR is the recommended report for monitoring program data quality. It touches on all areas of data quality and allows Agency Data Administrators an opportunity to simultaneously monitor project performance. The following reports should additionally be considered for monitoring data quality:

Agency Reports	Annual Performance Report (APR)/ESG CAPER	Data Quality Framework	Point-In-Time and Housing Inventory Reports	Project specific reports	Frequency
Data Completeness	x	x	x	x	Monthly or more frequently
Incongruities	x	x	x	x	Monthly or more frequently
Timeliness of Data Entry	x	x	x	x	Monthly or more frequently
Project Performance	x		x	x	Quarterly or more frequently

Section 3: Data Quality Plan

System data quality & performance is to be monitored by the HMIS Lead monthly. This may be done by requesting agencies to submit specified data quality reports and/or monitoring data quality directly in the system. The HMIS Lead should report any concerns to the Data & Performance Committee.

System Reports	Annual Performance Report (APR)	Data Quality Framework	Duplicate Client	User Last Login	Point-In-Time and Housing Inventory Reports	System Performance Measures	Longitudinal System Analysis (LSA)	Frequency
Data Quality	x	x	x		x	x	x	Quarterly or more frequently
System Utilization				x				Monthly or more frequently
System Performance		x			x	x	x	Semi-Annually or more frequently

Section 4: Security Plan

Introduction to the Homeless Management Information System Security Plan

Homeless Management Information System (HMIS) security standards are established to ensure the confidentiality, integrity, and availability of all HMIS information. The security standards are designed to protect against any reasonably anticipated threats or hazards to security and must be enforced by system administrators, agency administrators as well as end users. This section is written to comply with section 4.3 of the 2004 Homeless Management Information Systems (HMIS) Data and Technical Standards Final Notice (69 Federal Register 45888) as well as local legislation pertaining to maintaining an individual's personal information. I

Meeting the minimum standards in this Security Plan is required for participation in the HMIS. Any agency may exceed the minimum standards described in this plan and are encouraged to do so. All Agency Data Administrators are responsible for understanding this policy and effectively communicating the Security Plan to individuals responsible for security at their agency.

Security Plan Applicability

The HMIS and all agencies must apply the security standards addressed in this Security Plan to all the systems where personal protected information is stored or accessed. Additionally, all security standards must be applied to all networked devices. This includes, but is not limited to, an agency's networks, desktops, laptops, mobile devices, mainframes, and servers.

All agencies, including the HMIS Lead, will be monitored by the HMIS System Administrators annually to ensure compliance with the Security Plan. Agencies that do not adhere to the security plan will be given a reasonable amount of time to address any concerns. Egregious violations of the security plan may result in immediate termination of an agency or user's access to the HMIS as determined by the HMIS Lead.

System Security

User Authentication

Agency Data Administrators and System Administrators shall limit access to those who meet each of the following requirements:

- Access is required for the purpose of data assessment, entry, or reporting
- New User Training has been completed including the Standard Operating Procedures, Agency Privacy Policies, the Standard Workflow, and the overall HMIS software orientation.
- User is covered by the agency privacy notice
- User has signed and agreed to the HMIS End User Policy and Code of Ethics. HMIS End User Policy and Code of Ethics

- Have an agency email address to ensure HMIS access is granted to active employees only. Publicly available domain names are not appropriate (gmail.com, Hotmail.com, etc.) unless the agency uses these domain names as their agency standard.

It is the responsibility of Agency Data Administrators to provide 24-hour notice to the System Administrators when the person leaves or is scheduled to leave the agency or no longer requires access to the HMIS. Users who have not successfully logged into HMIS for 30 or more days may be inactivated by the System Administrator to further assure that access is only granted to those who require it.

The HMIS System only permits users to be logged into HMIS from one workstation or device at any given time.

User access and user access levels will be determined by the System Administrator in consultation with the Agency Data Administrator to ensure the correct level of access is provided for the user to complete their required tasks in the system.

Each user must have a unique user ID and password. The User ID and a default password will be set up by the System Administrator upon completion of training. The user will then use the “Forgot Password” feature in HMIS to establish a new password at initial log-in.

Passwords are the individual’s responsibility and must meet minimum system requirements, be kept secure, and be difficult to guess. **Users are prohibited from sharing user IDs or passwords.** If a user forgets their password or is locked out after multiple failed attempts, they may use the ‘forgot password’ feature in HMIS or contact the HMIS Help Desk for support, nilhmis.cayzu.com.

Passwords will expire every 45 days and users will be prompted upon log-in to reset their password. If a user has not logged into the system for more than 30 days, their account will be inactivated, and they will need to contact the HMIS Help Desk for support, nilhmis.cayzu.com.

Virus Protection

Industry-compliant virus protection software must be installed on all devices directly accessing the HMIS or accessing the HMIS via a network. The virus protection software must also include anti-spyware functionality.

Operating Systems must be supported by their vendors. Operating Systems and virus definitions must be set to be updated and applied automatically. Virus scans must be completed at least weekly.

Firewalls

An agency must protect the HMIS and client data from malicious intrusion behind a secure and up-to-date firewall. Each individual device does not need its own firewall if there is a firewall between that device and any systems, including the Internet and other computer networks, located outside of the organization. For example, a device that accesses the Internet through a modem, Wi-Fi or cellular data network would need its own firewall. A device that accesses the Internet through a central server would not need a firewall if the server has a firewall. Firewalls are commonly included with all new operating systems.

Physical Access

All computers and devices must be controlled through physical security measures and/or a password.

Users must logoff from the HMIS and their device if they leave their workstation. The HMIS System automatically logs users off after 30 minutes of inactivity. When devices are not in use, a password protected screensaver or lock screen should automatically turn on within 15 minutes of inactivity. Users on mobile devices or working in outreach locations in addition to system administrators are encouraged to decrease this time to 5 minutes.

Users should be trained on how to quickly lock their computer or device if they need to step away. On windows workstations, this is achieved by typing the command “Windows Key + L.” Different operating systems have different locking mechanisms.

If users are going to be away from the computer or device for an extended period of time, they are encouraged to shut down the computer or device. Users should follow their agency’s “shut-down procedures” to ensure proper device, network, and virus updates.

Disposal

Agency policies, consistent with applicable state and federal laws, should be established regarding appropriate locations for storage, transmission, use and disposal of HMIS generated hardcopy or digital data. Reasonable care should be used, and media should be secured when left unattended. Magnetic media containing HMIS data which is released and/or disposed of from the participating organization and central server should first be processed to destroy any data residing on that media. Degaussing and overwriting are acceptable methods of destroying data.

System Monitoring

The HMIS maintains an audit trail that tracks user log-in attempts and modifications to client records. Each audit entry reflects the user that created the entry and the date and name of the user that made the most recent modification.

These user logs will be checked routinely according to best practices established by the HMIS Lead Agency. Possible mechanisms the HMIS Lead may utilize are comparing the volume of search records accessed compared to the size of the agency, looking for multiple user logins from multiple locations, client searches occurring without record adjustment, users logging into the system at strange times and looking at the frequency of user password reset and lockout.

Hard Copy Data

Printed versions (hardcopy) of confidential data should not be left unattended and open to compromise. Media containing HMIS client identified data may not be shared with any person or agency other than the owner of the data for any reason not disclosed within the agency's Privacy Notice.

HMIS information in hardcopy format should be disposed of properly. This may include shredding finely enough to ensure that the information is unrecoverable.

Data Purge

Annually, Client records without any activity (program entries, needs, calls, case notes, etc.) for 7 or more years will be removed from HMIS by the software vendor.

Software Application Security

Disaster Recovery

The Northern Illinois (NIL) HMIS Technical Lead Agency is responsible for ensuring that its vendors meet all regulated Disaster Protection and Recovery requirements. NIL HMIS is covered under WellSky's "Basic Disaster Recovery Plan."

Electronic Data Transmission

The NIL HMIS Technical Lead Agency is responsible for ensuring that its vendors meet all regulated Electronic Data Transmission requirements.

Electronic Data Storage

The NIL HMIS Technical Lead Agency is responsible for ensuring that its vendors meet all regulated Electronic Data Storage requirements.

Workstation Minimum Requirements

Any computer that interfaces with the HMIS must meet the minimum specifications or functionality cannot be guaranteed. Three main factors that can impact system performance are data transfer efficiency, memory management, and machine speed. Currently, the requirements are as follows:

- Operating System - Windows 10 or 11
- Memory - 2GB RAM minimum, 4GB recommended
- Monitor - Screen Display - 1024 x 768 (XGA)
- Processor - Dual-Core processor
- Internet Connection - Broadband
- Internet Browsers: Google Chrome, Mozilla Firefox, MS Edge, Apple Safari.

There may be additional requirements for report creation.

Computer Crime

Computer crimes violate state and federal law. They include but are not limited to: unauthorized disclosure, modification or destruction of data, programs or hardware; theft of computer services; illegal copying of software; invasion of privacy; theft of hardware, software, peripherals, data or printouts; misuse of communication networks; promulgation of malicious software such as viruses; and breach of contract. Perpetrators may be prosecuted under state or federal law, held civilly liable for their actions, or both. The System Administrator and users must comply with license agreements for copyrighted software and documentation. Licensed software must not be copied unless the license agreement specifically provides for it. Copyrighted software must not be loaded or used on systems for which it is not licensed. All users agree to this upon logging into the system for the first time and accepting the software's *End User License Agreement*.

Illinois Personal Information Protection Act

As discussed in **Section 1** of this standard operating procedure, all agencies and users are bound to follow state and federal law and following those laws precede following this standard operating procedure. The steps outlined here are requirements of HMIS System Participation and should not be considered legal advice.

The Illinois Personal Information Protection Act (815 ILCS 530/5)[1] requires that data collectors who maintain Social Security numbers take sufficient measures to ensure the security of the data and to notify Illinois Residents if a data breach occurs. The collection of Social Security numbers is a mandatory requirement of HUD's minimum data collection requirements and thus both individual agencies as well as the HMIS are "Data Collectors" and are bound to the law. A client may be notified multiple times by each level of 'data holding' (HMIS Vendor, HMIS Lead, and individual agencies).

If a Breach Occurs at the Individual Agency

Upon detection of a breach of the security of the agency's data, the agency's Executive Director or Agency Data Administrator, must take the following actions:

1. Notification will be made to all Continuum of Care Contacts as listed on the Alliance to End Homelessness website, https://suburbancook.org/hmis.

2. Notification will be made to individual agency clients in **one** of the following ways
   a. Written notice
   b. Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures for notices legally required to be in writing as set forth in section 7001 of title 15 of the united states code[2]; or
   c. Substitute notice, if the data collector demonstrates that the cost of providing notice would exceed $250,000 or that the affected class of subject persons to be notified exceeds $500,000, or the data collector does not have sufficient contact information.

[1] http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=2702&ChapterID=67
[2] http://www.gpo.gov/fdsys/pkg/USCODE-2011-title15/pdf/USCODE-2011-title15-chap96-subchapI-sec7001.pdf

Substitute notice shall consist of all the following:

i. Email notice if the data collector has an email address for the subject persons;
ii. Conspicuous posting of the notice on the data collector's web site page if the data collector maintains one; and
iii. Notification to major statewide media

If Breach Occurs at a System Level

Upon detection of a breach of the security of the system data, the HMIS Lead must take the following actions:

1. Notification will be made to all Continuum of Care Contacts as listed on the Alliance to End Homelessness website, https://suburbancook.org/hmis.
2. Notify each participating agency's Agency Data Administrator and Executive Director
3. The HMIS does not maintain adequate records for individual notification if a breach occurs (current address, phone number or email address). Provide a substitute notification by completing all the following:
    a. Email Notice when an email address is available
    b. Conspicuous Posting to be added to the HMIS website
    c. Press Release to major statewide media

In either situation, the notice(s) must contain the following information:

1. The actual or approximate date of the security breach
2. The nature of the breach
3. A description of the steps that have or will be taken to address the breach
4. Toll-free number and address for each major consumer reporting agency and the Federal Trade Commission
5. Include a statement informing the individual that they can obtain information from each of the consumer reporting agencies about fraud alerts and security freezes.

Contact	Website	Phone	Address
Equifax	equifax.com/personal/credit-report-services	888-EQUIFAX (888-378-4329)	PO Box 740241 Atlanta, GA 30374
Transunion	transunion.com/credit-help	800-916-8800	PO Box 2000, Chester, PA 19022-2000
Experian	experian.com/help	888-EXPERIAN (888-397-	P.O. Box 4500, Allen, TX

		3742)	75013
Federal Trade Commission	https://reportfraud.ftc.gov/	877-FTC-HELP (877-382-4357)	600 Pennsylvania Ave., NW, Washington DC 20580

SAMPLE SECURITY BREACH NOTIFICATION LETTER

Date

Dear Recipient Name:

We are contacting you because we have learned of a serious data security incident that occurred on (specific or approximate date) *OR* between (date, year *and date, year)* that involved some of your personal information.

The breach involved (*provide a brief general description of the breach).* The information breached contained (*names, mailing addresses, and Social Security numbers, etc.*).

We are notifying you so you can take action along with our efforts to minimize or eliminate potential harm. [*describe action being taken*] Due to the serious nature of this incident, we strongly encourage you to take preventive measures to help prevent and detect any misuse of your information.

As a first preventive step, we recommend you closely monitor your financial accounts. If you see any unauthorized activity, promptly contact your financial institution. We also suggest you submit a complaint with the Federal Trade Commission, https://www.identitytheft.gov/, 600 Pennsylvania Avenue, NW, Washington, DC 20580, 877-FTC-HELP (877-382-4357).

As a second step, you also may want to contact the three U.S. credit reporting agencies (Equifax, Experian and TransUnion) to obtain a free credit report from each by calling 877-322-8228 or by logging onto www.annualcreditreport.com.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. A victim's personal information is sometimes held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

As a third step, you may want to contact the three U.S. credit reporting agencies to place the security freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze.

To obtain a security freeze, contact the following agencies:

Experian
P.O. Box 4500
Allen, TX 75013
888-397-3742
www.experian.com

Equifax
PO Box 740241
Atlanta, GA 30374
888-378-4329
www.equifax.com

TransUnion
PO Box 2000
Chester, PA 19022-2000
800-916-8800
www.transunion.com

If you have further questions or concerns, you may contact the undersigned at this special telephone number, 000-000-0000. You can also check our website at www.ourwebsite.org for updated information.

Sincerely,

Name

Title

Agency

DuPage County HMIS Standard Operating Procedures (SOP)
Summary of Updates for CoC Leadership Review and Approval
2024 Annual Review

Section 1: Roles and Responsibilities

Document/Section	Proposed Modifications
Introduction and Responsibilities	Added language to 2nd paragraph: "Agencies who receive funding through the following federal partners and their respective programs are to participate in their local HMIS: U.S. Department of Health and Human Services, U.S. Department of Housing and Urban Development, U.S. Department of Veteran Affairs, and any additional funding source requiring participation."
	Re-formatted documents into a table format.
	Updated Domestic Violence Service Providers to Victim Service Providers (VSP) throughout the SOP.
HMIS Partnership Agreement	None
Agency Data Administrator Acknowledgement	None
User Code of Ethics	Updated 1st Field to read: "HMIS User's First and Last Name" vs "HMIS Username".

Section 2: Privacy Plan

Document/Section	Proposed Modifications
Privacy Plan	Update to name of the formerly known as Data Sharing Refusal Form in the table and replacing refusal with "opt out or revoke" in the description.
	Removing redundant language "HMIS System" with just "HMIS" in the first paragraph. HMIS is Homeless Management Information System.
	Changing "and" to "or" in the 3rd paragraph, "Each agency must either adopt the Baseline Privacy Notice or develop a Privacy Notice which meets or exceeds all minimum requirements set forth in the Baseline Privacy Notice…"
Baseline Notice	Updated reference to the "Client Data Sharing Refusal Form" on bottom of page 2 under Your Rights Regarding Your Information in HMIS. "You have the right to opt-out of having your and your household members' information shared to partnering agencies in the Northeast Illinois Homeless Management Information System (HMIS). To do so, you must request and sign the "Request to Not Share Information in HMIS." Any information in the HMIS

	prior to signing the form will continue to be shared with the agencies as described in this notice.”
	Updated DuPage County Community Services to Northeast IL HMIS in last bullet point on bottom of page 2. “You may request a list of current HMIS partner organizations from [Agency Name], DuPage County Community Services, or review the current list at suburbancook.org/hmis. Northeast Illinois HMIS may add new HMIS partner organizations to this list at any time.”
Client Data Sharing Refusal Form	Updated name to “Request to Not Share Information in HMIS” and replacing the word “refuse” with decline or similar. This change was also made anywhere the name of the form is mentioned.
Acknowledgement of Receipt Form	Updated the name of the refusal form to the “Request to Not Share Information in HMIS” and related language. “If you would like a copy of the Privacy Notice or would like to request that your information is not shared in HMIS, please ask. Declining to sign this acknowledgement does not prevent us from using or disclosing your information. To prevent disclosure of your information in HMIS, you must complete the “Request to Not Share Information in HMIS” form. Your decision to not sign this acknowledgement will be documented along with the fact that you were informed of our Privacy Notice. “
	I was ~~given~~ advised of my rights including my rights ~~the option to request and sign the “Data Sharing Refusal Form.”~~to not share my information in HMIS.
Participating Agencies and Shared Information	None

Section 3: Data Quality Plan

Document/Section	Proposed Modifications
Data Quality Plan: Introduction to Data Quality	Simplified language throughout the Introduction and added language around using a client centered approach and tools that align with the standards. “Data quality in the Homeless Management Information System (HMIS) is crucial for accurately representing the reality of homelessness and program and system performance. To achieve good data quality, data must be assessed using a client centered approach, all tools must align with HMIS Data Standards and our local Data Quality Plan, and all data entry is to be completed in a timely fashion using a HMIS Staff approved workflow.”

Data Coverage	Updated Domestic Violence Provider to Victim Service Provider and added language around VSP project level data is captured in our CoCs HMIS.
	Re-worded the last paragraph to be more concise, "The Data & Performance Committee, along with the partnership of DuPage Continuum of Care's Leadership and related committees, will continue to assess community data needs, including the inclusion of new agencies and data elements."
Completeness	Added Agency Data Administrators to also be responsible for ensuring project data is accurate.
Data Quality Threshold Table	Added all required data elements for all project types and funding sources received in DuPage including the project level data. Thresholds only assigned to project level data for this must be 100% complete and accurate. Updated available reports as appropriate.
	Combined Race and Ethnicity
	Decrease Exit Destination threshold for Street Outreach from 40% to 21%. SO Destination was at 26%. Increase Income, Non-Cash, and Health Ins thresholds for both ES and SO from 10% to 50%. Where last reporting cycle ES was at 54% and SO 100% errors for Income at annual. *SO is only assessed on DQ when the client has an engagement date.
	Increase Income at Annual Threshold from 10 to 20% for all other HMIS projects.
	Separated Current Living Situation from Engagement (2 different data points).
	Removed Emergency Shelter Night by Night (ES nbn) since this is not a project type in DuPage CoC.
	Added Coordinated Entry data elements to table and included CE in the timeliness thresholds.
	Added a footnote that users should check with their funders if the full SSN is required.
Accuracy	Added language to provide more emphasis on entering data self-reported by the client and using client centered approaches when collecting information. Also emphasized the need to review data with the client at project start, update, annual and exit.
Consistency	Updated language to reflect entering client reported data and ensuring all tools meet the minimum data collection requirements.
Training	Proposal to remove the certification requirement with updated language, "Users will be expected to demonstrate understanding and proper data entry workflow prior to obtaining access to the live site. Alternative training modules may be required depending on the user's role and access in the system." *effects CoC scoring

	Update language around ADA Training requirements. "Agency Data Administrators or an agency/program representative shall participate in Agency Data Administrator trainings, and in turn relay this information, along with all other HMIS related updates, to the agency users." *effects CoC Scoring

Section 4: Security Plan

Document/Section	Proposed Modifications
Security Plan	"It is the responsibility of Agency Data Administrators to provide 24-hour notice to the System Administrators when the person leaves or is scheduled to leave the agency or no longer requires access to the HMIS."
	Proposed removal of "certification" requirement on pg 2. "Each user must have a unique user ID and password. The User ID and a default password will be set up by the System Administrator upon completion of training."
	Removal of the reference to Section 1 for I don't believe Section 1 delves into detail around user roles and assignment of licenses and added language as shown below. "User access and user access levels will be determined by the System Administrator in consultation with the Agency Data Administrator to ensure the correct level of access is provided for the user to complete their required tasks in the system."
	Added new section for the 7-year Data Purge.
Sample Letter-Breach	None