

HMIS POLICY COMMITTEE AGENDA
Wednesday 10/9/2019
2:00pm – 3:30 am

Location: 421 N. County Farm Rd.
Rm 3500-B

TOPIC	ACTION TO BE TAKEN	
1. Welcome	Meeting will be called to order at 2:00 p.m.	
2. Approval Minutes	Chair will ask for any additions or corrections of minutes from last HMIS Policy Committee meeting.	
3. Standard Operating Procedures	<i>Old Business</i>	<i>New Business</i>
	<ul style="list-style-type: none"> • HMIS Policy Committee positions still on hold...Leadership reviewing committee structure • 2019 Site Visits key findings • 2019 Annual End User re-certification training update 	<ul style="list-style-type: none"> • Review all sections of SOP for edits
4. Data Collection and System Wide Reporting	<i>Old Business</i>	<i>New Business</i>
	<ul style="list-style-type: none"> • Bed Inventory data collection • Review System Data (standing item) • Update on SP6 • Update on Qlik conversion 	<ul style="list-style-type: none"> • None
5. Announcements/Reminders	<ul style="list-style-type: none"> • CoC Leadership in process of reviewing governance structure 	
6. Future Meetings	Next Agency Data Administrator Training: <ul style="list-style-type: none"> • Friday, November 22nd, 2019 1:00pm – 2:00pm Next HMIS Policy Committee Meeting: <ul style="list-style-type: none"> • Wednesday, December 18th, 2019 2:00pm – 3:30pm 	

Attached:

- Minutes from June 2019 meeting
- HMIS Policy sections (all sections)

Meeting Date: 6/19/2019 **Meeting Time:** 2:00 p.m.

Meeting Location: Web Conference

Present: Will Moeller (Bridge), Julie Tremberth (HMIS), Samantha Concepcion (HMIS), Andy True (360), Tonya Latson (People’s Resource Center), Marisa Wiesman (Prairie State Legal Services)

Absent: Amy Palumbo, (Catholic Charities) Lisa Snipes (CoC), Becky Day (Health Department), Sara Vainowski (DuPagePads), Will Salmon (DuPagePads), Cate Croteau (Outreach Community Ministries)

Agenda Items	Discussion	Conclusion	Next Steps
1. Welcome & Introductions	Meeting called to order at 2:05pm	M. Wiesman now representing Prairie State Legal Services.	She will join the committee officially soon
2. Approval Minutes	Minutes distributed by W. Moeller by email prior to meeting.	No comments on minutes.	Minutes sent to leadership.
3. Standard Operating Procedures	<p>Old Business</p> <ul style="list-style-type: none"> • HMIS Policy Committee Positions on hold. Leadership reviewing committee structure. <p>New Business</p> <ul style="list-style-type: none"> • Site Visit Progress • 2020 HUD HMIS Data Standards Released 	<p>Old Business</p> <p>New Business</p> <ul style="list-style-type: none"> • HMIS emailed Site Visit emails last week. They are to be completed by 8/31/2019. • HMIS will go over data quality, compliance, and HMIS licenses needed for each agency. • Main Data Standards changes: <ul style="list-style-type: none"> ○ Project level changes for System Admins ○ Minor picklist/workflow changes for programs and users ○ Addition of Coordinated Entry data standards into the manual. These standards are not required (though strongly encouraged) since DuPage’s CE is not funded by HUD. 	<p>Old Business</p> <ul style="list-style-type: none"> • HMIS will be working on training so that end users will be prepared for these changes. • Coordinated Entry committee will speak on the impact of these changes.
4. Data Collection and System Wide Reporting	<p>Old Business</p> <ul style="list-style-type: none"> • Review System Data (standing item) ○ New concerns due to programming changes 	<p>Old Business</p> <ul style="list-style-type: none"> • S. Concepcion shared systemwide 0640 reports. • Same fields to work on: Destination, Income <ul style="list-style-type: none"> ○ Reports now using Client Location and Head of Household Relationship field to filter clients. Clients with errors in these fields are being kicked out of the report. 	<ul style="list-style-type: none"> ○ HMIS to focus on Client Location, HoH Relationship, and RRH Move-In Date in ADA

	<p>New Business</p> <ul style="list-style-type: none"> • System Performance Measure submission • Longitudinal Statistical Analysis (LSA) submission 	<ul style="list-style-type: none"> ○ RRH is required to put a client move-in date once they move in to PH, regardless of whether they were housed by the RRH program. <p>New Business</p> <ul style="list-style-type: none"> • SPM Submitted. System Admins had to do data corrections for Head of Household and Client Location for data to come in correctly. • New final deadline of 6/24/2019. • Only one DQ flag for Exit Destination which is expected due to our night by night shelter. • Currently no errors on the QC report being flagged, only warnings. • All tables are currently marked as usable. • HUD has come out with a new data analysis tool called Stella which will use LSA data to create dashboards. 	<p>trainings and New End User trainings.</p> <ul style="list-style-type: none"> • HMIS will submit the LSA by 6/24/2019
<p>5. Announcements & Reminders</p>	<ul style="list-style-type: none"> • CoC Leadership in process of reviewing governance structure • Update Qlik conversion <ul style="list-style-type: none"> ○ Training next week with partners in Suburban Cook on Qlik. • ServicePoint 6 <ul style="list-style-type: none"> ○ Had a call with WellSky where they showed HMIS Team their roadmap for April to June. <ul style="list-style-type: none"> ▪ The first change was the Password Reset which has already taken effect in our system. ▪ The next change will be ShelterPoint, which our community currently does not use. HMIS will evaluate the new ShelterPoint and based on the changes in the module may suggest its use to our shelters. ○ Call next week with WellSky regarding Open Referral API. 		
<p>6. Future Meetings</p>	<p>Next Agency Data Administrator Training: Friday, July 26th, 2019 1:00 pm – 2:00 pm</p> <p>Next HMIS Policy Committee Meeting: Wednesday, August 21st, 2019 2:00 pm – 3:30 pm</p>		

Prepared and Submitted by: Samantha Concepcion
Reviewed by:

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.

The DuPage County Continuum of Care participates in the “Northeast Illinois HMIS” (NIL HMIS). The NIL HMIS is a shared, regional HMIS which multiple CoCs participate in and is managed by a single Technical Lead Agency.

This document provides the policies and procedures that govern the DuPage County Continuum of Care Homeless Management Information System and all local system administrators and participating agencies. They are collectively referred to as the Standard Operating Procedures (SOPs). The SOPs have been developed in order to comply with HUD regulations, state and federal laws and also to retain consistency in developing and maintaining the HMIS.

Responsibilities

The HMIS Team is composed of the Alliance to End Homelessness in Suburban Cook County, the DuPage County Community Services Department, the DuPage County CoC Leadership Committee, the DuPage County CoC HMIS Policy Committee, Participating Agencies and Agency Data Administrators.

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.

There are three documents which formalize the responsibilities of all members of the HMIS Team:

Memorandum of Understanding between and amongst the Cook County Continuum of Care, the DuPage County Continuum of Care, DuPage County and the Alliance to End Homelessness in Suburban Cook County

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.

DuPage County Homeless Continuum of Care Governance Charter for the Homeless Management Information System (HMIS)

This document designates the DuPage County Department of Community Services as the HMIS Lead and describes its responsibilities as the HMIS Lead

HMIS Partner Agreement between DuPage County Community Services and [Participating Agency]

This document describes the responsibilities of participating agencies and their users.

Summary of DuPage County Responsibilities:

Northeast Illinois HMIS Governing Forum: this forum will facilitate collaborative and consensus driven decision making on implementation-wide governance areas.

Northeast Illinois HMIS Technical Lead Agency: currently designated as the Alliance to End Homelessness in Suburban Cook County, this agency is responsible for the overall coordination, implementation and execution of the HMIS on behalf of the partner Continuums of Care.

DuPage County Continuum of Care Leadership Committee: this committee oversees the DuPage County HMIS Lead and is primarily responsible for all local HMIS activity.

DuPage County HMIS Policy Committee: this committee reports to the DuPage County Continuum of Care Leadership Committee and is responsible for developing and reviewing HMIS policies and procedures and cultivating ways in which data measurement can contribute to providing visionary data leadership.

DuPage County HMIS Lead: currently designated as the DuPage County Community Services Department, the HMIS lead guides the local operation of the HMIS implementation within DuPage County.

Participating HMIS Agency & Users: participating agencies and affiliated users provide services to individuals in DuPage County and record those services and client information into the HMIS in accordance with these SOPs.

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 outlined 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 System. 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 an open system of client-level data sharing amongst 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 and 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 approved by the HMIS Committee of the DuPage County Continuum of Care.

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.
Client Data Sharing Refusal Form	This form gives the client the opportunity to refuse the sharing of their information to other agencies within the system.	*REQUIRED* -if adopting baseline privacy notice* If the agency adopts the baseline privacy notice, they 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	*Optional* Agencies are encouraged, but not required to utilize this form.

their rights regarding opting-out of data sharing.

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, HIPPA 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)

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 II" 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] PRIVACY NOTICE

Effective (05/01/2015)

Version 3.0

THIS NOTICE DESCRIBES HOW INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

A. What This Notice Covers

1. This notice describes the privacy policy and practices of [Name of Agency]. Our main office is at [Address, web address, telephone contact information].
2. A client is anyone whose personal data is included in the Northeast Illinois HMIS [in connection with the receipt of services or assistance]. This person need not be homeless.
3. When a client request services from this agency, we enter information about them and members of their household into a computer system called a Homeless Management Information System (HMIS). This HMIS is used by many agencies in Suburban Cook and DuPage Counties that provide services to persons and families in need.
4. The HMIS is administered by DuPage County Department of Community Services. Their office is at 421 N County Farm Road, Wheaton, IL 60187. Their website is www.dupageco.org/HMIS. You can contact the system administrator at 630-407-6397. DuPage County Department of Community Services has adopted this Privacy Notice as well.
5. The policy and practices in this notice cover the processing of protected personal information of those agencies participating in the Northeast Illinois Homeless Management Information System (HMIS). All personal information that we maintain, not just the information entered into the HMIS, is covered by the policy and practices described in this notice. This policy covers only the programs within the agency that participate in HMIS.
6. Protected Personal information (PPI) is any information we maintain about a client that:
 - a. allows identification of an individual directly or indirectly
 - b. can be manipulated by a reasonably foreseeable method to identify a specific individual, **or**
 - c. can be linked with other available information to identify a specific client.When this notice refers to personal information, it means PPI.
7. We adopted this policy because of standards for Homeless Management Information Systems issued by the Department of Housing and Urban Development. We intend our policy and practices to be consistent with those standards. See 69 Federal Register 45888 (July 30, 2004).
8. This notice tells our clients, our staff, and others how we process personal information. We follow the policy and practices described in this notice.
9. We may amend this notice and change our policy or practices at any time. Amendments may affect personal information that we obtained before the effective date of the amendment. All amendments are approved by the HMIS Committee of the DuPage County Continuum of Care and are then adopted by all agencies that use the HMIS.

Current information about the DuPage County HMIS Committee can be found on the HMIS website at www.dupageco.org/HMIS.

10. We give a written copy of this privacy notice to any individual who asks. We maintain a copy of this policy on the HMIS website at www.dupageco.org/HMIS.

B. How and Why We Collect Personal Information

1. We collect personal information only when appropriate to provide services or for another specific purpose of our agency or when required by law.
2. We may collect personal information for these purposes:
 - a. To provide or coordinate services to clients
 - b. To locate other programs that may be able to assist clients
 - c. To verify information given to us by clients
 - d. For functions related to payment or reimbursement from other services that we provide
 - e. To operate our agency, including administrative functions such as legal, audits, personnel, oversight, and management functions
 - f. To comply with reporting obligations
 - g. When required by law
3. We may be required to collect some personal information by law or by organizations that give us money to operate this program. Other personal information that we collect is important to run our programs, to improve services, and to better understand the need individuals in the community. We only collect information that we consider to be appropriate.
4. We only use lawful and fair means to collect personal information.
5. We normally collect personal information with the knowledge or consent of our clients. If you seek our assistance and provide us with personal information, we assume that you consent to the collection of information as described in this notice.
6. We may also get personal information from:
 - a. Individuals who are with you or are part of your household
 - b. Individuals who are assisting you
 - c. Individuals or organizations you provide for verification of information or references
 - d. Information already collected about you by other agencies that are part of the HMIS
 - e. Other private organizations in the DuPage County Continuum of Care
 - f. Government agencies including DuPage County and the State of Illinois.
 - g. Public records including internet searches, telephone directories and other published sources
7. When possible, we post a sign at our intake desk or other location explaining the reasons we ask for personal information. The sign gives our agency's contact information, the HMIS administrator's contact information and the location of this privacy notice.

C. How We Use and Disclose Personal Information

1. We use or disclose personal information for activities described in this part of the notice. We may or may not make any of these uses or disclosures with your information. We share client records with other agencies that may have separate privacy policies and that may allow different uses and disclosures of the information.

2. All participating agencies of the Northeast Illinois HMIS share client record information. The information that is shared with these participating agencies is extensive. The list of these agencies and the information shared changes frequently. You can view a full list of these agencies and the information that we share at our website, www.dupageco.org/HMIS.
3. **You have the right to opt-out of having this information shared with other participating agencies.** To do so, you must request and sign the “Client Data Sharing Refusal Form.” If you sign this form, your information will remain in the HMIS and be subject to the other disclosures in this privacy notice, but the information will not be available to the other participating agencies of the Northeast Illinois HMIS.
4. The information that will be shared if you do not opt-out is as follows:
 - a. Personal identification information
 - b. Demographic information
 - c. Program Enrollment Type and Dates
 - d. The name of your case manager, if you are assigned one

The detailed list of information that we share can be found at our website:
www.dupageco.org/HMIS

5. Some programs and agencies require sharing of information different than what is discussed in this privacy notice. For those programs, individuals will be presented with additional consent information.
6. We assume that you consent to the use or disclosure of your personal information for the purposes described here and for other uses and disclosures that we determine to be compatible with these uses or disclosures:
 - a. to provide or coordinate services to individuals
 - b. for functions related to payment or reimbursement for services
 - c. to carry out administrative functions such as legal, audits, personnel, oversight, and management functions
 - d. to create de-identified (anonymous) information that can be used for research and statistical purposes without identifying clients
 - e. when required by law to the extent that use or disclosure complies with and is limited to the requirements of the law, including Freedom of Information Act requests
 - f. to avert a serious threat to health or safety if
 - (1) we believe that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public, and
 - (2) the use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat
 - g. to report about an individual we reasonably believe to be a victim of abuse, neglect or domestic violence to a governmental authority (including a social service or protective services agency) authorized by law to receive reports of abuse, neglect or domestic violence
 - (1) under any of these circumstances:
 - (a) where the disclosure is required by law and the disclosure complies with and is limited to the requirements of the law
 - (b) if the individual agrees to the disclosure, or

- (c) to the extent that the disclosure is expressly authorized by statute or regulation, and
 - (I) we believe the disclosure is necessary to prevent serious harm to the individual or other potential victims, or
 - (II) if the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the PPI for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.
- (2) when we make a permitted disclosure about a victim of abuse, neglect or domestic violence, we will promptly inform the individual who is the victim that a disclosure has been or will be made, except if:
 - (a) we, in the exercise of professional judgment, believe informing the individual would place the individual at risk of serious harm, or
 - (b) we would be informing a personal representative (such as a family member or friend), and we reasonably believe the personal representative is responsible for the abuse, neglect or other injury, and that informing the personal representative would not be in the best interests of the individual as we determine in the exercise of professional judgment.
- h. for academic research purposes
 - (1) conducted by an individual or institution that has a formal relationship with this agency if the research is conducted either:
 - (a) by an individual employed by or affiliated with the organization for use in a research project conducted under a written research agreement approved in writing by a designated agency program administrator (other than the individual conducting the research), or
 - (b) by an institution for use in a research project conducted under a written research agreement approved in writing by a designated agency program administrator.
 - (2) any written research agreement:
 - (a) must establish rules and limitations for the processing and security of PPI in the course of the research
 - (b) must provide for the return or proper disposal of all PPI at the conclusion of the research
 - (c) must restrict additional use or disclosure of PPI, except where required by law
 - (d) must require that the recipient of data formally agree to comply with all terms and conditions of the agreement, and
 - (e) is not a substitute for approval (if appropriate) of a research project by an Institutional Review Board, Privacy Board or other applicable human subjects protection institution.
- i. to a law enforcement official for a law enforcement purpose (if consistent with applicable law and standards of ethical conduct) under any of these circumstances:
 - (1) in response to a lawful court order, court-ordered warrant, subpoena or summons issued by a judicial officer, or a grand jury subpoena

- (2) if the law enforcement official makes a written request for PPI that:
 - (a) is signed by a supervisory official of the law enforcement agency seeking the PPI
 - (b) states that the information is relevant and material to a legitimate law enforcement investigation
 - (c) identifies the PPI sought
 - (d) is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought, and
 - (e) states that de-identified information could not be used to accomplish the purpose of the disclosure.
 - (3) if we believe in good faith that the PPI constitutes evidence of criminal conduct that occurred on our premises
 - (4) in response to an oral request for the purpose of identifying or locating a suspect, fugitive, material witness or missing person and the PPI disclosed consists only of name, address, date of birth, place of birth, Social Security Number, and distinguishing physical characteristics, or
 - (5) the official is an authorized federal official seeking PPI for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879 (threats against the President and others), and the information requested is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought.
 - j. to comply with reporting obligations for homeless management information systems and for oversight of compliance with homeless management information system requirements.
 - k. to the administrators and contractors of the HMIS system, including DuPage County and Suburban Cook County Staff and contractors, Bowman Systems, L.L.C staff and contractors and the HMIS Committee Chairperson and vice-Chairperson.
7. Before we disclose your personal information that is not described here, we seek your consent first.

D. How to Inspect and Correct Personal Information

1. You may inspect and have a copy of your personal information that we maintain. We will offer to explain any information that you may not understand.
2. We will consider a request from you for correction of inaccurate or incomplete personal information that we maintain about you. If we agree that the information is inaccurate or incomplete, we may delete it or we may choose to mark it as inaccurate or incomplete and to supplement it with additional information.
3. To inspect, get a copy of, or ask for correction of your information, ask a program staff member how to obtain this information.
4. We may deny your request for inspection or copying of personal information if:
 - a. the information was compiled in reasonable anticipation of litigation or comparable proceedings
 - b. the information is about another individual (other than a health care provider or homeless provider)
 - c. the information was obtained under a promise or confidentiality (other than a promise from a health care provider or homeless provider) and if the disclosure would reveal the source of the information, **or**

- d. disclosure of the information would be reasonably likely to endanger the life or physical safety of any individual.
5. If we deny a request for access or correction, we will explain the reason for the denial. We will also include, as part of the personal information that we maintain, documentation of the request and the reason for the denial
6. We may reject repeated or harassing requests for access or correction.

E. Data Quality

1. We collect only personal information that is relevant to the purposes for which we plan to use it. To the extent necessary for those purposes, we seek to maintain only personal information that is accurate, complete, and timely.
2. We are developing and implementing a plan to dispose of personal information, found in the HMIS system, not in current use seven years after the information was created or last changed. As an alternative to disposal, we may choose to remove identifiers from the information.
3. We may keep information for a longer period if required to do so by statute, regulation, contract, or other requirement.

F. Complaints and Accountability

1. We accept and consider questions or complaints about our privacy and security policies and practices. Because there are many agencies and parties involved, it is often hard to know where to direct a complaint. We ask that questions or complaints regarding the HMIS go to the HMIS System Administrator at DuPage County Community Services. Questions or complaints pertaining to the agency serving you should follow the agency's grievance procedure. If you are unsure where to go, you may go to either agency listed below and we will help you determine the best person to speak with.

HMIS System Administrator

421 N County Farm Road

Wheaton, IL 60187

630-407-6397

www.dupageco.org/HMIS

[Agency Contact Information]

[Address]

[Address]

[Phone Number]

[Website]

2. All members of our staff (including employees, volunteers, affiliates, contractors and associates) are required to comply with this privacy notice. Each staff member must receive and acknowledge receipt of a copy of this privacy notice.

G. Change History:

1. Version 1.0 October 2009- Initial Policy was a part of client consent documents
2. Version 2.0 October 2012 - Adopted HUD's baseline privacy notice and detailed our implied consent disclosure process
3. Version 3.0 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.

Section 3- Data Quality Plan

Introduction to Data Quality

Data quality refers to the extent that data recorded in HMIS accurately reflects the same information in the real world. To meet the HMIS goal of reporting on the extent and nature of homelessness, it is critical that HMIS has the best possible representation of reality as it relates to homeless people and the programs that serve them. Specifically, it should be our goal to record the most accurate, consistent and timely information to draw reasonable conclusions about the extent of homelessness and the impact of homeless services. To best ensure we are achieving good data quality, all data entry must be captured using a HMIS Staff approved workflow.

Data elements included in this Data Quality Plan are determined by the US Department of Housing and Urban Development (HUD), all Federal Partners, and the DuPage Continuum of Care. This plan is written to comply with the most recent version of the HMIS Data Standards Manual and Data Dictionary¹. The HMIS Data Standards Manual and Data Dictionary describe what information must be collected, for which projects, persons and at which point in time. This section is not intended to replace the details of that document but to establish local thresholds for data quality errors based on program and funding type.

The Data Quality Plan applies to all participating HMIS projects regardless of project type or funding source, but some data elements may only be required for specific project types as noted in the table below. Not all data elements will be included in this plan, and projects should be mindful to routinely review their program manuals² for further guidance.

The HMIS Policy Committee is responsible for reviewing this Data Quality Plan annually.

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, excluding any domestic violence provider. Domestic Violence providers' bed coverage data will be submitted to HMIS annually or more frequently as needed. The Bed Coverage Rate is calculated by project type,

$$= \frac{\text{\# dedicated homeless beds in DuPage CoC HMIS}}{\text{\# dedicated homeless beds in the DuPage CoC}}$$

Other

The HMIS Committee, along with the partnership of the Continuum of Care's Leadership and Needs Assessment

¹ <https://www.hudexchange.info/resource/3824/hmis-data-dictionary/>

² <https://www.hudexchange.info/programs/hmis/hmis-guides/#coc-resources>

Committees, will continue to evaluate the data needs of the community and will address those needs as appropriate, including but not limited to the inclusion of new HMIS participating agencies, the inclusion of new data elements, and the furthering of current data analysis.

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 Staff are to ensure that the [Project Descriptor Data Elements](#) are complete for all homeless system³ and prevention⁴ projects and that the data is reviewed annually for each project with each Agency Data Administrator.
- Each HMIS 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 Rate⁵ less than the amount as specified in the [Data Quality Error Rate Thresholds Table](#)

Data Quality Error Rate Thresholds

Element Type	Data Element	Project Type	Client	Collection Point	Error Rate Threshold	Tools to Measure
Universal Data Element	Name and Name Data Quality	All	All	Record Creation	5%	<ul style="list-style-type: none"> – Data Quality Framework – APR – ESG CAPER
Universal Data Element	Social Security Number (SSN) and SSN Data Quality	All	All	Record Creation	10%	<ul style="list-style-type: none"> – Data Quality Framework – APR – ESG CAPER
Universal Data Element	Date of Birth and Date of Birth Data Quality	All	All	Record Creation	5%	<ul style="list-style-type: none"> – Data Quality Framework – APR – ESG CAPER
Universal Data Element	Race	All	All	Record Creation	5%	<ul style="list-style-type: none"> – Data Quality Framework – APR – ESG CAPER
Universal Data Element	Ethnicity	All	All	Record Creation	5%	<ul style="list-style-type: none"> – Data Quality Framework – APR – ESG CAPER

³ Homeless System Project must meet the following:

- The primary intent of the project is to serve homeless persons
- The project verifies homeless status as part of its eligibility determination
- The actual project clients are predominantly homeless (or, for permanent housing, were homeless at entry).

Homelessness is to be defined by the Homeless Emergency Assistance and Rapid Transition to Housing (HEARTH), where at this time Category 3 is not approved by HUD.

⁴ Homelessness Prevention Project is a project that offers services and/or financial assistance necessary to prevent a person from moving into an emergency shelter or place not meant for human habitation.

⁵ Error Rate includes null, don't know/refused, and incongruent data

Section 4- Security Plan

Introduction to the HMIS Security Plan

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. In December 2013, HUD released proposed regulations pertaining to HMIS Security. These regulations are not yet in force and sufficient guidance has not been given to enact the policies.

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 System 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 –

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

5. 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 immediately inactivate a user and notify System Administrators when the person leaves 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. The roles and responsibilities pertaining to assignment and creation of user licenses are outlined in *Section 1: Roles and Responsibilities*.

Each user must have a unique user ID. Each user's identity will be authenticated using a user password. Passwords are the individual's responsibility. **Users are prohibited from sharing user IDs or passwords.** A temporary password will be automatically generated from the system when a new user is created. Agency Data Administrators or System Administrators will communicate the system-generated password to the user. The user will be asked to establish a permanent password at initial log-in.

Users must select and change their own passwords every forty-five days. A password cannot be consecutively re-used. Password format is case-sensitive and must be between eight and sixteen characters long including at least two numbers and not be easily guessed. Any passwords written down must be securely stored and inaccessible to other persons. If a user unsuccessfully attempts to logon three times, the user ID will be "locked out", access permission revoked, and the user will be unable to gain access until their password is reset.

Agency Data Administrators and System Administrators have permission to reset a user's password. Users may submit a Help-Desk request for assistance, www.dupageco.org/HMISHelp.

Virus Protection

All devices directly accessing the HMIS and any device that is on a network that has a device directly accessing the HMIS must have industry compliant virus protection software installed. Both Operating System updates and virus definitions must be set to be updated and applied automatically. The virus protection software must also include anti-spyware functionality. Operating Systems must be supported by their vendors. 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, as long as 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, public 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 as long as 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 a permanent 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.

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. Currently the vendor commits itself to the following:

- Nightly database tape backups.
- Offsite storage of tape backups
- 7-day backup history stored locally on instantly accessible Raid 10 storage
- 1-month backup history stored off site
- 24 x 7 accesses to emergency line to provide assistance related to “outages” or “downtime”.
- 24 hours backed up locally on instantly-accessible disk storage

Electronic Data Transmission

The NIL HMIS Technical Lead Agency is responsible for ensuring that its vendors meet all regulated Electronic Data Transmission requirements. Currently the vendor commits itself to the following:

- 128-bit SSL encryption is used to encrypt client data as it travels "over the wire" from the vendor's data center to the user's desktop.

Electronic Data Storage

The NIL HMIS Technical Lead Agency is responsible for ensuring that its vendors meet all regulated Electronic Data Storage requirements. Currently the vendor commits itself to the following:

- Data is stored in a binary format utilizing PostgreSQL data base application.
- Data is encrypted annually to provide an additional level of security.

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 7, 8, and 10

Memory

- 2GB RAM minimum, 4GB recommended

Monitor

- Screen Display - 1024 x 768 (XGA)

Processor

- Dual-Core processor

Internet Connection

Broadband

- Internet Browsers in order of compatibility: Google Chrome, Mozilla Firefox, Internet Explorer, Apple Safari.

There are additional requirements for the report creation functionality of the HMIS.

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 One** 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 [HMIS website](#)²
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](#)³; 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. Substitute notice shall consist of all of the following:
 - (1) Email notice if the data collector has an email address for the subject persons;
 - (2) Conspicuous posting of the notice on the data collector's web site page if the data collector maintains one; **and**

(3) 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 [HMIS website](#)²
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 of 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 (appendix xx)
5. Toll-free number, address and website for the Federal Trade Commission (appendix xx)
6. Include a statement informing the individual that they can obtain information from each of the consumer reporting agencies about fraud alerts and security freezes.

¹ <http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=2702&ChapterID=67>

² http://www.dupageco.org/Community_Services/Community_Development/HMIS/35384/

³ <http://www.gpo.gov/fdsys/pkg/USCODE-2011-title15/pdf/USCODE-2011-title15-chap96-subchapl-sec7001.pdf>

Universal Data Element	Gender	All	All	Record Creation	5%	<ul style="list-style-type: none"> – Data Quality Framework – APR – ESG CAPER
Universal Data Element	Veteran Status	All	All	Record Creation	10%	<ul style="list-style-type: none"> – Data Quality Framework – APR – ESG CAPER
Universal Project Stay Element	Disabling Condition (Y/N)	All	All	Project Start	10%	<ul style="list-style-type: none"> – Data Quality Framework – APR – ESG CAPER
Universal Project Stay Element	Project Start Date	All	All	Project Start	10%	<ul style="list-style-type: none"> – Data Quality Framework – APR – ESG CAPER
Universal Project Stay Element	Destination at Exit	NBN ES and SO	All	Project Exit	40%	<ul style="list-style-type: none"> – Data Quality Framework – APR – ESG CAPER
Universal Project Stay Element	Destination at Exit	All but NBN ES and SO	All	Project Exit	10%	<ul style="list-style-type: none"> – Data Quality Framework – APR – ESG CAPER
Universal Project Stay Element	Relationship to Head of Household	All	All	Project Start	10%	<ul style="list-style-type: none"> – Data Quality Framework – APR – ESG CAPER
Universal Project Stay Element	Client Location	All	Head of Household	Project Start, Update	10%	<ul style="list-style-type: none"> – Data Quality Framework – APR – ESG CAPER
Universal Project Stay Element	Living Situation: Residence Prior	All	Head of Household, Adults	Project Start	10%	<ul style="list-style-type: none"> – APR – ESG CAPER
Universal Project Stay Element	Living Situation: Chronic Homeless Status	All	Head of Household, Adults	Project Start	10%	<ul style="list-style-type: none"> – Data Quality Framework – APR – ESG CAPER
Program Specific Data Element	Income	All, but NBN ES	Head of Household, Adults	Project Start, Update, Annual, Exit	10%	<ul style="list-style-type: none"> – Data Quality Framework – APR – ESG CAPER
Program Specific	Non-Cash Benefits	All, but NBN ES	Head of Household, Adults	Project Start, Update, Annual, Exit	10%	<ul style="list-style-type: none"> – Data Quality Framework – APR – ESG CAPER

Program Specific	Health Insurance	All, but NBN ES	All	Project Start, Update, Annual, Exit	10%	<ul style="list-style-type: none"> – APR – ESG CAPER
Program Specific	Disability	All	All	Project Start, Update, Exit	10%	<ul style="list-style-type: none"> – APR – ESG CAPER
Program Specific	Domestic Violence	All	Head of Household, Adults	Project Start, Update	10%	<ul style="list-style-type: none"> – APR – ESG CAPER
Program Specific	Contacts and Engagement	NBN ES and SO	Head of Household, Adults	Occurrence Point	10%	<ul style="list-style-type: none"> – ESG CAPER
Program Specific	Bed Nights	NBN ES	All	Occurrence Point	10%	<ul style="list-style-type: none"> – ES-DQ- Services to Exit Trifecta – ESG CAPER
Program Specific	Percent of AMI	All	Head of Household, Adults	Project Start, Update, Annual, Exit	10%	<ul style="list-style-type: none"> – Basic Demographic and EE Details – SSVF Export (for SSVF projects only)

Timeliness

To ensure accuracy of our data at any given time, HMIS data entry is to be completed within 10 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: 11+ Days	Tools to Measure
Program Start	A Program Start Date will be created within 10 days of 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	All	25%	<ul style="list-style-type: none"> – Data Quality Framework – APR – ESG CAPER

	eligibility determination (PH).			
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	25%	<ul style="list-style-type: none"> – Data Quality Framework – APR – ESG CAPER
Program Exit	A Program Exit Date will be recorded in HMIS within 10 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, but NBN ES and SO	Not Available	<p>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.</p> <p>We recommend agencies to utilize current report to spot check for accurate service and bed utilization. Those reports include:</p> <ul style="list-style-type: none"> – Data Quality Framework – APR – ESG CAPER
Program Exit	A Program Exit Date will be recorded in HMIS within 10 days of learning of the client leaving the program, or when it has been 30 days since the last Shelter Stay (NBN) or Contact (SO). The Exit Date will be equal to the last day of shelter (NBN) or Contact (SO).	NBN ES, SO	Not Available	<p>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.</p> <p>We recommend agencies to utilize current report to spot check for accurate service and bed utilization. Those reports include:</p>

				<ul style="list-style-type: none"> – ESG CAPER – Trifecta
--	--	--	--	---

Accuracy

We cannot assume that all information given to us by clients is truthful or that all data is always entered correctly. Inaccurate data may be intentional or unintentional. In general, false or inaccurate information is worse than incomplete information, since with the latter, it is at least possible to acknowledge the gap. Thus, it should be emphasized to clients and staff that it is better to enter nothing (or preferably “Data not collected”) 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 made a Universal Intake form available online, www.dupageco.org/HMIS.
- Review data quality and program specific reports for inaccurate information (pregnant males, minor veterans, etc.)
- Ensure the client understands what is being asked of them, what their options are, and that staff do not stray from the intent of the question.
- Audit a random sample of client records
- Review answers to questions with clients at subsequent interactions, at minimum on an annual basis.
- Ensure accurate project start, annual review, and exit dates for all participants. (See Timeliness Threshold Table).

Annually, System Administrators will audit a random selection of client files during the HMIS site visit to assess for tools that align with the required data elements and whether this data is accurately captured at all required points in time (program Start, Annual and Exit). A list of client Id’s will be provided in advance of the visit to each agency.

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 a 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 and the Standard Workflow, in addition to any project specific information.

New users may take a self-guided online End User certification exam that covers topics from the new user training. Users must obtain a 75% or better to pass the test. While this exam is not a requirement for accessing the system, agencies are encouraged to have at least 50% of their users pass the certification test.

To stay current and maintain access to HMIS, all Users must complete an annual re-training provided by System Administrators. Training topics will vary each year depending on the needs of the system.

Agency Data Administrators or an agency/program representative must attend all scheduled Agency Data Administrator trainings, and in turn relay this 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 generate system-level reports is dependent upon a common definition of fields, question wording and data entry/workflow. It is up to each agency to ensure adherence to HMIS Staff approved workflows.

Monitoring Data Quality

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

Agency/Program data quality is to be monitored by the Agency Data Administrator on a monthly basis. 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.

As a guideline, the HUD CoC APR is the recommended report for monitoring agency data quality. It touches on all areas of data quality and also 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

System data quality & performance is to be monitored by the HMIS Lead on a monthly basis. 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 HMIS Policy Committee.

System Reports	Annual Performance Report (APR)	Data Quality Framework	Duplicate Client	User Last Login	System Growth Reports	Point-In-Time and Housing Inventory Reports	System Performance Measures	Longitudinal System Analysis (LSA)	Other reports as needed	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	x	-	Semi-Annually or more frequently



HMIS End User Policy and Code of Ethics

HMIS User Name (Please Print)

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 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 any 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 HMIS Notice of Privacy Practices and the <i>HMIS Standard Operating Procedures</i> , 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 Executive Director, if Agency Data Administrator is unavailable or if the Executive Director is otherwise the most appropriate contact. The Agency Data Administrator and Executive Director are responsible for taking action 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.



HMIS End User Policy and Code of Ethics

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 to the following:

Passwords are your responsibility and you may not share passwords. They should be securely stored and inaccessible to other persons—including your supervisor(s). Passwords should never be stored or displayed in any publicly accessible location and should not be transmitted electronically without the DuPage System Administrator's permission.

USER GRIEVANCE PROCEDURE

If you have a grievance with this Code of Ethics, you may send a written complaint to this Agency.

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 System Administrator.

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
HMIS User Login (Username)	
Email Address	
Agency/System Administrator Signature	Date



HMIS Agency Data Administrator Policy and Code of Ethics

Agency Data Administrator Name (Please Print)

Responsibilities of each Agency Data Administrator

The Executive Director of each Participating Agency will appoint a qualified person as the Agency Data Administrator, who will need to ensure participation in all Agency Data Administrator trainings.

The Agency Data Administrator will be responsible for:

(Initial each line below)

	Acting as the key point-person with all information regarding HMIS and their designated agency.
	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.
	Reviewing and coordinating with HMIS System Administrators to update agency information in the HMIS database.
	Managing technical access to HMIS for authorized persons
	Notifying HMIS Staff of user changes as soon as possible, at minimum 24 hours after their occurrence
	Training new staff persons on the uses of the DuPage County Continuum HMIS including review of the SOPs in this document and any agency policies which impact the security and integrity of client information
	Ensuring that unsupervised access to the DuPage County Continuum HMIS be granted to authorized staff members only after they have received training and satisfactorily demonstrated proficiency in use of the software and understanding of the SOPs and agency policies referred to above
	Notifying all users in their agency of interruptions to service
	Generating reports for agency specific data, when needed. This includes reviewing reports to ensure data integrity, data quality, full reporting of HUD Minimum Data Requirements & other data required by the agency to complete reports, etc.
	Attending training to ensure ongoing understanding of the development of the HMIS, improved technical reporting capabilities, system updates, etc.
	Implementing an Agency data security policy and standards, including: <ul style="list-style-type: none"> ▪ 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

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

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 “Client 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 the “Client Data Sharing Refusal Form,” please ask.

Refusing to sign this acknowledgement does not prevent us from using or disclosing your information. In order to prevent disclosure of your information to, you must request and sign the “Client Data Sharing Refusal Form.” If you refuse to sign this acknowledgement, we will keep a record that you refused to sign the acknowledgement but 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 have 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 given the option to request and sign the “Client Data Sharing Refusal Form.”
- I understand that services cannot be denied to me because of my refusal to share my information.

Name of Client or Guardian

Signature of Client or Guardian

Date

[AGENCY] PRIVACY NOTICE

Effective (05/01/2015)

Version 3.0

THIS NOTICE DESCRIBES HOW INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

A. What This Notice Covers

1. This notice describes the privacy policy and practices of [Name of Agency]. Our main office is at [Address, web address, telephone contact information].
2. A client is anyone whose personal data is included in the Northeast Illinois HMIS [in connection with the receipt of services or assistance]. This person need not be homeless.
3. When a client request services from this agency, we enter information about them and members of their household into a computer system called a Homeless Management Information System (HMIS). This HMIS is used by many agencies in Suburban Cook and DuPage Counties that provide services to persons and families in need.
4. The HMIS is administered by DuPage County Department of Community Services. Their office is at 421 N County Farm Road, Wheaton, IL 60187. Their website is www.dupageco.org/HMIS. You can contact the system administrator at 630-407-6397. DuPage County Department of Community Services has adopted this Privacy Notice as well.
5. The policy and practices in this notice cover the processing of protected personal information of those agencies participating in the Northeast Illinois Homeless Management Information System (HMIS). All personal information that we maintain, not just the information entered into the HMIS, is covered by the policy and practices described in this notice. This policy covers only the programs within the agency that participate in HMIS.
6. Protected Personal information (PPI) is any information we maintain about a client that:
 - a. allows identification of an individual directly or indirectly
 - b. can be manipulated by a reasonably foreseeable method to identify a specific individual, **or**
 - c. can be linked with other available information to identify a specific client.When this notice refers to personal information, it means PPI.
7. We adopted this policy because of standards for Homeless Management Information Systems issued by the Department of Housing and Urban Development. We intend our policy and practices to be consistent with those standards. See 69 Federal Register 45888 (July 30, 2004).
8. This notice tells our clients, our staff, and others how we process personal information. We follow the policy and practices described in this notice.
9. We may amend this notice and change our policy or practices at any time. Amendments may affect personal information that we obtained before the effective date of the amendment. All amendments are approved by the HMIS Committee of the DuPage County Continuum of Care and are then adopted by all agencies that use the HMIS.

Current information about the DuPage County HMIS Committee can be found on the HMIS website at www.dupageco.org/HMIS.

10. We give a written copy of this privacy notice to any individual who asks. We maintain a copy of this policy on the HMIS website at www.dupageco.org/HMIS.

B. How and Why We Collect Personal Information

1. We collect personal information only when appropriate to provide services or for another specific purpose of our agency or when required by law.
2. We may collect personal information for these purposes:
 - a. To provide or coordinate services to clients
 - b. To locate other programs that may be able to assist clients
 - c. To verify information given to us by clients
 - d. For functions related to payment or reimbursement from other services that we provide
 - e. To operate our agency, including administrative functions such as legal, audits, personnel, oversight, and management functions
 - f. To comply with reporting obligations
 - g. When required by law
3. We may be required to collect some personal information by law or by organizations that give us money to operate this program. Other personal information that we collect is important to run our programs, to improve services, and to better understand the need individuals in the community. We only collect information that we consider to be appropriate.
4. We only use lawful and fair means to collect personal information.
5. We normally collect personal information with the knowledge or consent of our clients. If you seek our assistance and provide us with personal information, we assume that you consent to the collection of information as described in this notice.
6. We may also get personal information from:
 - a. Individuals who are with you or are part of your household
 - b. Individuals who are assisting you
 - c. Individuals or organizations you provide for verification of information or references
 - d. Information already collected about you by other agencies that are part of the HMIS
 - e. Other private organizations in the DuPage County Continuum of Care
 - f. Government agencies including DuPage County and the State of Illinois.
 - g. Public records including internet searches, telephone directories and other published sources
7. When possible, we post a sign at our intake desk or other location explaining the reasons we ask for personal information. The sign gives our agency's contact information, the HMIS administrator's contact information and the location of this privacy notice.

C. How We Use and Disclose Personal Information

1. We use or disclose personal information for activities described in this part of the notice. We may or may not make any of these uses or disclosures with your information. We share client records with other agencies that may have separate privacy policies and that may allow different uses and disclosures of the information.

2. All participating agencies of the Northeast Illinois HMIS share client record information. The information that is shared with these participating agencies is extensive. The list of these agencies and the information shared changes frequently. You can view a full list of these agencies and the information that we share at our website, www.dupageco.org/HMIS.
3. **You have the right to opt-out of having this information shared with other participating agencies.** To do so, you must request and sign the “Client Data Sharing Refusal Form.” If you sign this form, your information will remain in the HMIS and be subject to the other disclosures in this privacy notice, but the information will not be available to the other participating agencies of the Northeast Illinois HMIS.
4. The information that will be shared if you do not opt-out is as follows:
 - a. Personal identification information
 - b. Demographic information
 - c. Program Enrollment Type and Dates
 - d. The name of your case manager, if you are assigned one

The detailed list of information that we share can be found at our website:
www.dupageco.org/HMIS

5. Some programs and agencies require sharing of information different than what is discussed in this privacy notice. For those programs, individuals will be presented with additional consent information.
6. We assume that you consent to the use or disclosure of your personal information for the purposes described here and for other uses and disclosures that we determine to be compatible with these uses or disclosures:
 - a. to provide or coordinate services to individuals
 - b. for functions related to payment or reimbursement for services
 - c. to carry out administrative functions such as legal, audits, personnel, oversight, and management functions
 - d. to create de-identified (anonymous) information that can be used for research and statistical purposes without identifying clients
 - e. when required by law to the extent that use or disclosure complies with and is limited to the requirements of the law, including Freedom of Information Act requests
 - f. to avert a serious threat to health or safety if
 - (1) we believe that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of an individual or the public, and
 - (2) the use or disclosure is made to a person reasonably able to prevent or lessen the threat, including the target of the threat
 - g. to report about an individual we reasonably believe to be a victim of abuse, neglect or domestic violence to a governmental authority (including a social service or protective services agency) authorized by law to receive reports of abuse, neglect or domestic violence
 - (1) under any of these circumstances:
 - (a) where the disclosure is required by law and the disclosure complies with and is limited to the requirements of the law
 - (b) if the individual agrees to the disclosure, or

- (c) to the extent that the disclosure is expressly authorized by statute or regulation, and
 - (I) we believe the disclosure is necessary to prevent serious harm to the individual or other potential victims, or
 - (II) if the individual is unable to agree because of incapacity, a law enforcement or other public official authorized to receive the report represents that the PPI for which disclosure is sought is not intended to be used against the individual and that an immediate enforcement activity that depends upon the disclosure would be materially and adversely affected by waiting until the individual is able to agree to the disclosure.
- (2) when we make a permitted disclosure about a victim of abuse, neglect or domestic violence, we will promptly inform the individual who is the victim that a disclosure has been or will be made, except if:
 - (a) we, in the exercise of professional judgment, believe informing the individual would place the individual at risk of serious harm, or
 - (b) we would be informing a personal representative (such as a family member or friend), and we reasonably believe the personal representative is responsible for the abuse, neglect or other injury, and that informing the personal representative would not be in the best interests of the individual as we determine in the exercise of professional judgment.
- h. for academic research purposes
 - (1) conducted by an individual or institution that has a formal relationship with this agency if the research is conducted either:
 - (a) by an individual employed by or affiliated with the organization for use in a research project conducted under a written research agreement approved in writing by a designated agency program administrator (other than the individual conducting the research), or
 - (b) by an institution for use in a research project conducted under a written research agreement approved in writing by a designated agency program administrator.
 - (2) any written research agreement:
 - (a) must establish rules and limitations for the processing and security of PPI in the course of the research
 - (b) must provide for the return or proper disposal of all PPI at the conclusion of the research
 - (c) must restrict additional use or disclosure of PPI, except where required by law
 - (d) must require that the recipient of data formally agree to comply with all terms and conditions of the agreement, and
 - (e) is not a substitute for approval (if appropriate) of a research project by an Institutional Review Board, Privacy Board or other applicable human subjects protection institution.
- i. to a law enforcement official for a law enforcement purpose (if consistent with applicable law and standards of ethical conduct) under any of these circumstances:
 - (1) in response to a lawful court order, court-ordered warrant, subpoena or summons issued by a judicial officer, or a grand jury subpoena

- (2) if the law enforcement official makes a written request for PPI that:
 - (a) is signed by a supervisory official of the law enforcement agency seeking the PPI
 - (b) states that the information is relevant and material to a legitimate law enforcement investigation
 - (c) identifies the PPI sought
 - (d) is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought, and
 - (e) states that de-identified information could not be used to accomplish the purpose of the disclosure.
 - (3) if we believe in good faith that the PPI constitutes evidence of criminal conduct that occurred on our premises
 - (4) in response to an oral request for the purpose of identifying or locating a suspect, fugitive, material witness or missing person and the PPI disclosed consists only of name, address, date of birth, place of birth, Social Security Number, and distinguishing physical characteristics, or
 - (5) the official is an authorized federal official seeking PPI for the provision of protective services to the President or other persons authorized by 18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22 U.S.C. 2709(a)(3), or for the conduct of investigations authorized by 18 U.S.C. 871 and 879 (threats against the President and others), and the information requested is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought.
 - j. to comply with reporting obligations for homeless management information systems and for oversight of compliance with homeless management information system requirements.
 - k. to the administrators and contractors of the HMIS system, including DuPage County and Suburban Cook County Staff and contractors, Bowman Systems, L.L.C staff and contractors and the HMIS Committee Chairperson and vice-Chairperson.
7. Before we disclose your personal information that is not described here, we seek your consent first.

D. How to Inspect and Correct Personal Information

1. You may inspect and have a copy of your personal information that we maintain. We will offer to explain any information that you may not understand.
2. We will consider a request from you for correction of inaccurate or incomplete personal information that we maintain about you. If we agree that the information is inaccurate or incomplete, we may delete it or we may choose to mark it as inaccurate or incomplete and to supplement it with additional information.
3. To inspect, get a copy of, or ask for correction of your information, ask a program staff member how to obtain this information.
4. We may deny your request for inspection or copying of personal information if:
 - a. the information was compiled in reasonable anticipation of litigation or comparable proceedings
 - b. the information is about another individual (other than a health care provider or homeless provider)
 - c. the information was obtained under a promise or confidentiality (other than a promise from a health care provider or homeless provider) and if the disclosure would reveal the source of the information, **or**

- d. disclosure of the information would be reasonably likely to endanger the life or physical safety of any individual.
5. If we deny a request for access or correction, we will explain the reason for the denial. We will also include, as part of the personal information that we maintain, documentation of the request and the reason for the denial
6. We may reject repeated or harassing requests for access or correction.

E. Data Quality

1. We collect only personal information that is relevant to the purposes for which we plan to use it. To the extent necessary for those purposes, we seek to maintain only personal information that is accurate, complete, and timely.
2. We are developing and implementing a plan to dispose of personal information, found in the HMIS system, not in current use seven years after the information was created or last changed. As an alternative to disposal, we may choose to remove identifiers from the information.
3. We may keep information for a longer period if required to do so by statute, regulation, contract, or other requirement.

F. Complaints and Accountability

1. We accept and consider questions or complaints about our privacy and security policies and practices. Because there are many agencies and parties involved, it is often hard to know where to direct a complaint. We ask that questions or complaints regarding the HMIS go to the HMIS System Administrator at DuPage County Community Services. Questions or complaints pertaining to the agency serving you should follow the agency's grievance procedure. If you are unsure where to go, you may go to either agency listed below and we will help you determine the best person to speak with.

HMIS System Administrator

421 N County Farm Road

Wheaton, IL 60187

630-407-6397

www.dupageco.org/HMIS

[Agency Contact Information]

[Address]

[Address]

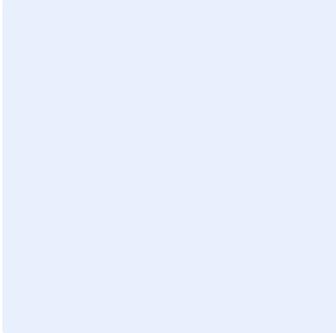
[Phone Number]

[Website]

2. All members of our staff (including employees, volunteers, affiliates, contractors and associates) are required to comply with this privacy notice. Each staff member must receive and acknowledge receipt of a copy of this privacy notice.

G. Change History:

1. Version 1.0 October 2009- Initial Policy was a part of client consent documents
2. Version 2.0 October 2012 - Adopted HUD's baseline privacy notice and detailed our implied consent disclosure process
3. Version 3.0 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.



DuPage County Homeless Management Information System

This posting summarizes how information about you may be used and disclosed and how you can get access to this information.

Agency use of your information	<ul style="list-style-type: none"> • We collect personal information for reasons that are discussed in our Privacy Notice. • We may be required to collect some personal information by law or by organizations that give us money to operate this program. • Other personal information that we collect is important to run our programs, to improve services, and to better understand the need individuals in the community. • We only collect information that we consider to be appropriate. • We assume that you consent to the use or disclosure of your personal information as described in the Privacy Notice. 	
Your rights and choices	<ul style="list-style-type: none"> • You have the right to request a copy of the Privacy Notice and have your questions answered. • You have the right to refuse to answer any question we ask, though this may impair our ability to provide the services you are requesting. • You have the right to opt-out of having your information shared with other agencies by requesting and signing the “Client Data Sharing Refusal Form.” 	
Contact information	[Agency Contact Info]	<p>DuPage County HMIS System Administrator 421 N County Farm Road Room 3-100 Wheaton, IL 60187 www.dupageco.org/HMIS 630-407-6397</p>

**To read the full Privacy Notice, ask for a copy or visit
[\[www.dupageco.org/HMIS\]](http://www.dupageco.org/HMIS)**