

HMIS Agency Data Administrator Training

Friday, January 25

1:00 pm – 2:30 pm

421 N County Farm Rd.

Wheaton, IL

Conference Room 3500B

Presenters:







Julie Tremberth and Samantha Concepcion

Attendees:

See Attached Sign-in Sheet

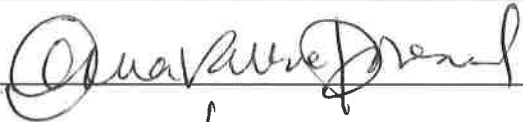
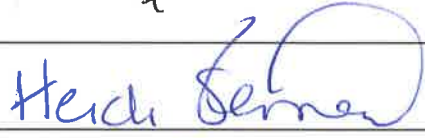
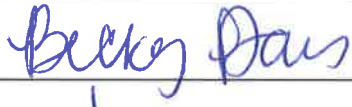
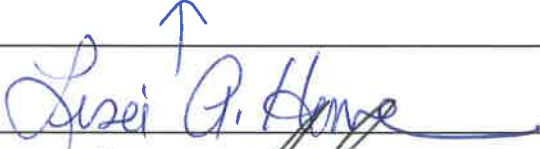

Introductions & Agenda Review	<ul style="list-style-type: none">• Notes are also available online for review, http://www.dupageco.org/HMIS
Updates	<ul style="list-style-type: none">• SOP Changes<ul style="list-style-type: none">– No changes to “Section 1 – Roles & Responsibilities” and “Section 2 – Privacy Plan”– “Section 3 – Data Quality Plan”: New error threshold chart– “Section 4 – Security Plan”: Broadened language to include all devices• Training Updates<ul style="list-style-type: none">– End User Part 1 training to be updated to reflect SOP changes, ready by early February– Next End User Part 2 training on February 15th– Report training to be scheduled quarterly. Next training in April– Coordinated Entry training now available on HMIS website– Recorded trainings and End User Certification exam are now hosted on SurveyMonkey.• Qlik and ServicePoint 6<ul style="list-style-type: none">– WellSky devoted more resources to Qlik and ServicePoint 6– HMIS System Admins do not expect transition to happen soon; will keep ADAs updated.• LSA (formerly known as the AHAR)<ul style="list-style-type: none">– “Final submission” sent in for our CoC. We are now waiting for contact from a HUD TA to further work on our submission.– Programming issues on WellSky’s and HUD’s ends still to be worked out
Common Questions/Concerns	<ul style="list-style-type: none">• Ensure users at agencies are explaining the privacy policy well to clients• Common data issues<ul style="list-style-type: none">– Sub-assessments (incongruent and null data)– Completeness issues<ul style="list-style-type: none">▪ Data Quality fields (like for Social Security Number and Name) left blank▪ Not answering all Domestic Violence questions▪ Not answering all Living Situation questions▪ Not updating active client records if there are data standard changes▪ Users not reviewing information that is already on the assessment for accuracy▪ Users not completing all assessments

<p>Reports/Data Needs</p>	<ul style="list-style-type: none"> • PIT and HIC Supplement (Public Folder -> 02 DuPage -> Program Type Specific Reports -> PIT/HIC) <ul style="list-style-type: none"> – Most updated reports in PIT/HIC folder. WellSky to release new version of 0630-Sheltered-Unsheltered PIT report in early February. No word on a new version of 0628-HIC Supplement. – “If yes, expected to be of long-continued and indefinite duration and substantially impairs ability to live independently” from Disability Sub-Assessment now pulling into several calculations in the reports. – For the 0628-HIC Supplement: <ul style="list-style-type: none"> ▪ Report only counts those with a valid move-in date ▪ In client detail tab (Tab D), there is an input control that allows you to see all clients in the program, not just those with a valid move-in date. • Provider Admin Survey (Public Folder -> 02 DuPage -> Program Type Specific Reports -> PIT/HIC) <ul style="list-style-type: none"> – Review/update information for all of your agency’s projects • Coordinated Entry Reports (SSO, EE) now available. (Public Folder -> 02 DuPage -> Program Type Specific Reports -> Coordinated Entry) <ul style="list-style-type: none"> – Fill in the Coordinated Entry provider in the EDA Provider prompts • The Emergency Shelter Quad-Shooter is now the Quintuplet! (Public Folder -> 02 DuPage -> Data Quality -> Other Data Quality Reports) <ul style="list-style-type: none"> – Added a check for Duplicate services for one shelter night. • 0252 – Data Completeness Report Card is back! (Public Folder -> 02 DuPage -> Data Quality -> Monthly Data Quality Reports) • Demo: Services Dashboard (Public Folder -> 01 Regional Share) <ul style="list-style-type: none"> – Provides graphics and counts of clients and services given
<p>Next Meeting</p>	<ul style="list-style-type: none"> • March 22 @ 1:00 pm 3500B

Program	Signature
360 Youth Services	
360 Youth Services - Cornerstone Group Home for Boys	
360 Youth Services - Cornerstone Group Home for Boys (ES)	
360 Youth Services - DuPage Young Women's Transitional Housing	
360 Youth Services - LGBTQ Transitional Housing	
360 Youth Services - Young Men's Transitional Housing (CoC TH)	
360 Youth Services - Young Men's Transitional Housing (IDHS TH)	
Bridge Communities - Children's Program	
Bridge Communities - Education Program	
Bridge Communities - Employment Program	
Bridge Communities - Interview Process	
Bridge Communities - Nutrition Services	
Bridge Communities - Pathways	
Bridge Communities - Phone Intakes	
Bridge Communities - Transitional Housing (HP)	
Catholic Charities, Diocese of Joliet	
Catholic Charities - DuPage Daybreak (HUD)	 
Catholic Charities - Emergency Services-Homeless Prevention	
Catholic Charities-ESG-County-HP	
Catholic Charities-ESG-County-RRH	

Catholic Charities-ESG-State-RRH	<p><i>Amy Lozano</i></p>	
Catholic Charities - First Light (PSH)		
Catholic Charities - Hope House (ES)		
Catholic Charities-IDHS-HP		
Catholic Charities-IDHS-RRH		
Catholic Charities-Other-HP		
Catholic Charities-Other-RRH		
Catholic Charities - Partners In Housing (PSH)		
Catholic Charities-SHIFT (PSH)		
Catholic Charities-TBRA HP		
Catholic Charities-TBRA RRH		
Catholic Charities-Transitional Housing		
DuPage County Community Services		<p><i>Veronica Jarama</i></p>
DuPage County Community Services-Case Management		
DuPage County Community Services-Case Management-CSBG FSS	<p><i>Amy Lozano</i></p>	
DuPage County Community Services-Homeless Prevention Program		
DuPage County Community Services-Homeless Prevention Program-CSBG-HP		
DuPage County Community Services-Homeless Prevention Program-CSBG-RRH		
DuPage County Community Services-Homeless Prevention Program-ESG-County-HP		
DuPage County Community Services-Homeless Prevention Program-ESG-County-RRH		
DuPage County Community Services-Homeless Prevention Program-ESG-State-RRH		

DuPage HMIS Agency Data Administrator Training

DuPage County Community Services-Homeless Prevention Program-IDHS-HP	
DuPage County Community Services-Homeless Prevention Program-IDHS-RRH	
DuPage County Community Services-Homeless Prevention Program-Other-HP	
DuPage County Community Services-Homeless Prevention Program-Other-RRH	
DuPage County Community Services-IDHS-SHP	
DuPage County Health Department	
DuPage County Health Department-Housing Intensive Services (PSH)	
DuPage County Health Department-MISA-CAP (PSH)	
DuPage County Health Department-SAIL (PSH)	
DuPage Housing Authority (HMIS)	
DuPage Housing Authority (HMIS) - VASH (PSH)	
DuPagePads	
DuPagePads - Carol's Place (PSH)	
DuPagePads - Case Management	
DuPagePads - Client Service Center	
DuPagePads - Employment Services	
DuPagePads - Family Outreach Program	
DuPagePads - Homecomings (PSH)	
DuPagePads - Housing Now (RRH)	
DuPagePads - Interim (overnight) Housing	
DuPagePads - Liberty Place (PSH)	

DuPagePads - Medical Respite Outreach	
DuPagePads - New Horizons (PSH)	
DuPagePads - Olympus Place (PSH)	
DuPagePads - Partners In Housing (PSH)	
DuPagePads - Pathways (PSH)	
DuPagePads - Stepping Stones (PSH)	
DuPagePads - Street Outreach	
DuPagePADS-TBRA HP	
DuPagePADS-TBRA RRH	
Midwest Shelter for Homeless Veterans - Captain Kevin C. Landeck Freedom Commissary	
Midwest Shelter for Homeless Veterans-Emergency Services-Other HP	
Midwest Shelter for Homeless Veterans-Emergency Services-Other RRH	
Midwest Shelter for Homeless Veterans - Employment Program	
Midwest Shelter for Homeless Veterans- Freedom Harbour (PSH)	
Midwest Shelter for Homeless Veterans - Miller Affordable Housing	
Midwest Shelter for Homeless Veterans - Supportive Services for Veteran Families	
Midwest Shelter for Homeless Veterans - Tammy's Trace	
MSHV-GPD Bridge Beds (TH)	
MSHV-GPD Low Demand (SH)	
MSHV-SSVF-DuPage-HP	
MSHV-SSVF-DuPage-RRH	

OCM-OCC-ESG-County-HP	<i>Bridget Adegbenro</i> 
OCM-OCC-ESG-County-RRH	
OCM-OCC-ESG-State-RRH	
OCM-OCC-IDHS-HP	
OCM-OCC-IDHS-RRH	
OCM-OCC-Other-HP	
OCM-OCC-Other-RRH	
OCM-Outreach Community Center	
OCM-Outreach Community Center-Homeless Prevention	
OCM-Warrenville Youth and Family Services	
OCM-Warrenville Youth and Family Services-Homeless Prevention	
OCM-Wheaton Youth Outreach	
OCM-Wheaton Youth Outreach-Homeless Prevention	
OCM-WYFS-ESG-County-HP	
OCM-WYFS-ESG-County-RRH	
OCM-WYFS-ESG-State-RRH	
OCM-WYFS-IDHS-HP	
OCM-WYFS-IDHS-RRH	
OCM-WYFS-Other-HP	
OCM-WYFS-Other-RRH	
OCM-WYO-ESG-County-HP	

OCM-WYO-ESG-County-RRH	Bridget Adegbenro	
OCM-WYO-ESG-State-RRH		
OCM-WYO-IDHS-HP		
OCM-WYO-IDHS-RRH		
OCM-WYO-Jubilee Village TH		
OCM-WYO-Other-HP		
OCM-WYO-Other-RRH		
OCM-WYO - Transitions TH		
Outreach Community Ministries		
People's Resource Center		Called In/Attended GoToMeeting JL
People's Resource Center-Homelessness Prevention		Kerry O'Hara
People's Resource Center-Homelessness Prevention-ESG-County-HP		
People's Resource Center-Homelessness Prevention-ESG-County-RRH		
People's Resource Center-Homelessness Prevention-ESG-State-RRH		
People's Resource Center-Homeless Prevention-EFSP-HP		
People's Resource Center-Homeless Prevention-EFSP-RRH		
People's Resource Center-Homeless Prevention-IDHS-HP		
People's Resource Center-Homeless Prevention-IDHS-RRH		
People's Resource Center-Homeless Prevention-Other-HP		
People's Resource Center-Homeless Prevention-Other-RRH		
Prairie State Legal Services		

DuPage HMIS Agency Data Administrator Training

Prairie State Legal Services-CDBG	Kerag & Brie
Prairie State Legal Services-CSBG	↓
Prairie State Legal Services-ESG-County-Homeless Legal Assistance	
Serenity House Counseling Services, Inc.	Called In/Attended GoToMeeting JL
Serenity House Counseling Services, Inc. Extended Residential Care Program-Non-State Beds	↓
Serenity House Counseling Services, Inc. Extended Residential Care Program-State Beds	
Serenity House Counseling Services, Inc. Recovery Homes	Stacy J. JB
Veterans Assistance Commission of DuPage County	
YWCA of Metropolitan Chicago - Patterson and McDaniel Family Center	

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

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

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>