Data & Performance Committee Agenda
Wednesday 5/5/2021
1:30pm – 2:50 pm

Location: Virtual via Microsoft Teams

TOPIC	ACTION TO BE TAKEN
Welcome	Meeting will be called to order at 1:30 p.m.
1. Approval Minutes	Chair will ask for any additions or corrections of minutes from last HMIS Policy Committee meeting (10/2020).
2. Leadership Updates	• Approved SOP, including new privacy plan • Data reports on the regular to Leadership meetings • Staffing of HMIS team at DuPage and Alliance to End Homelessness
3. Check-in	Conversation about - How are you doing? What pressure level are you feeling at your agency? How has data utilization changed or evolved at your agency during COVID?
4. New Privacy Notice, question about disclosure to law enforcement	Brief conversation about law enforcement disclosures (attachments)
5. Create plan to implementation	• Create schedule of upcoming tasks (e.g. HMIS annual system changes, bylaw approvals, etc.) • Sign up for work related to objectives, which include creating benchmarks for objectives and action plans for objectives.
Tentative items:	• System DQ reports (if available) • Julie to present recommendations on implementation of new privacy notice
Announcements/ Reminders	
Future Meetings	Next **Agency Data Administrator** Training: • Friday, May 28th at 1:00 pm Next **Data & Performance Committee** Meeting: • Wednesday, June 9th at 2:00 pm

Attached:

- Minutes from October 2020 meeting
- Comparison of Our Privacy Language vs. Federal Registry
- New privacy notice
- HUD Data Standards with highlights
- Re-worded strategies and objectives
- Tentative items, if available:
    - System data quality reports (coming via email prior to meeting)

Meeting Date: **6/17/2020** **Meeting Time: 2:00 pm**

Meeting Location: **Webinar – meetings.ringcentral.com**

Present: Will Moeller (Bridge), Julie Tremberth (HMIS), Samantha Concepcion (HMIS), Lisa Snipes (CoC), Marisa Wiesman (PSLS), Amy LaFauce (Catholic Charities), Cate Croteau (OCM), Kat Gilman (Midwest Shelter); Adam Swilley (DuPage PADS), Kelly Mannion – 360

Agenda Item	Discussion	Conclusion	Next Steps
Welcome & Introductions	Meeting called to order at 2 pm		
1. Approval of Minutes	Minutes distributed by W. Moeller by email prior to the meeting.	No comments on minutes.	Minutes will be sent to Leadership.
2. Updates	• All of the CoC committees now have chairs and will have a meeting in next two months • PADS has a hired a new director – Adam Swilley.	We are tabling reaching out to committee chairs for information needs.	Revisit contacting chairs at a future date.
3. Compliance Matters COVID-19's impact on HMIS SOP Compliance Site visits (include reference to security violation(s) from SOP in packet)	Julie & Sam will still be doing compliance visits but they will be virtual. Focus to date has been on making sure everyone has the right security in place when working remotely. They did inactivate users if no activity for 30 days. To reinstate, notify the Help Desk.		If anyone has a user who has been deactivated, have them contact the Help Desk.
4. P.E.M.D.A.S. Review the order of operations for D&P in determining policy and strategy	Our purpose is to have local compliance with the HUD HMIS data standards. Adding more data standards can put bigger picture at risk.	We need to have data in the best condition possible, as our data goes to the Feds and then Congress. Data also goes to the VA. Discussion reviewed the objectives Will had	We will start by introducing new Committee Chairs to what data/reports are currently available to them. Will bring Julie's outline to Leadership.

		provided under the categories of Reporting, Operations and Utilization. Members also expressed a need for educational objectives and wondered where that could fit in. Objective feasibility was discussed and suggestions made. Qlik is not yet available but will provide deep data for users.	The objectives will be reworked by Will and Kat based on comments and will be presented at the next meeting. HMIS System Administrators will also be involved.
5. Data Story for CoC System admins will share brief purpose statement of reports used by CoC	Discussion centered around how each agency uses the Data in HMIS.	Local agencies use data for a variety of purposes, including for reporting, need based data for grants, etc. A few agencies have multiple reporting systems for their programs besides HMIS. Local leadership can use reports to set local direction	
6. Who Cares? CoC Lead Agency explained how HMIS Data is used in funding	How we currently meet HUD's data requirements were discussed.	We do well overall but need to improve on exit destination and timeliness (Annual reviews specifically). High error rates require an explanation in Federal reporting (Exit Destination is high due to having a Night-by-night shelter). The CoC's timeliness threshold for data entry recently decreased.	Julie wants agencies to use canned APR/ESG CAPER reports and the 0640 - HUD Data Quality Report Framework to help check and correct some of the Data Quality errors. The old APR Data quality report in ART is no longer valid.
7. Activity	Strategic Activity	Tabled	

8. Announcements/ Reminders	Bridge Communities announced their new CEO. DuPage PADS CEO search status
9. Future Meetings	Next **Agency Data Administrator** Training: • Friday, July 24, 2020 - 1:00 pm Next **Data & Performance Committee** Meeting: • Wednesday, August 19th, 2020 - 2:00pm – 3:30pm
10. Meeting Adjourned	The meeting adjourned at 3:26

Prepared and submitted by: Cate Croteau

Reviewed by: Will Moeller

Our Language in current Privacy Practices
RE: Law enforcement

Law enforcement officials, but the disclosure must meet the minimum standards necessary for the immediate purpose and not disclose information about other individuals. A court order or search warrant may be required.

Language found in Federal Registry 59(146)

Uses and disclosures required by law. A CHO may use or disclose PPI when required by law to the extent that these or disclosure complies with and is limited to the requirements of the law.

Uses and disclosures to avert a serious threat to health or safety. A CHO may, consistent with applicable law and standards of ethical conduct, use or disclose PPI if: (1) The CHO, in good faith, believes 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 toa person reasonably able to prevent or lessen the threat, including the target of the threat.

Language in Federal Registry 69(146)
RE: HMIS Data & Technical Standards Final Notice

Disclosures for law enforcement purposes. A Covered Homeless Organization (CHO) may, consistent with applicable law and standards of ethical conduct, disclose Protected Personal Information (PPI) for a law enforcement purpose to a law enforcement official under any of the following circumstances:

- In response to a lawful court order, court-ordered warrant, subpoena or summons issued by a judicial officer, or a grand jury subpoena;
- If the law enforcement official makes a written request for protected personal information that: (1) Is signed by a supervisory official of the law enforcement agency seeking the PPI; (2)states that the information is relevant and material to a legitimate law enforcement investigation; (3) identifies the PPI sought; (4) is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and (5)states that de-identified information could not be used to accomplish the purpose of the disclosure.
- If the CHO believes in good faith that the PPI constitutes evidence of criminal conduct that occurred on the premises of the CHO;
- 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
- If (1) the official is an authorized federal official seeking PPI for the provision of protective services to the President or other persons authorized by18 U.S.C. 3056, or to foreign heads of state or other persons authorized by 22U.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 (2) the information requested is specific and limited in scope to the extent reasonably practicable in light of the purpose

1. Protected Personal Information (PPI). Any information maintained by or for a Covered Homeless Organization about a living homeless client or homeless individual that: (1) Identifies, either directly or indirectly, a specific individual; (2) can be manipulated by a reasonably foreseeable method to identify a specific individual; or (3) can be linked with other available information to identify a specific individual.

2. Covered Homeless Organization (CHO). Any organization (including its employees, volunteers, affiliates, contractors, and associates) that records, uses or processes PPI on homeless clients for an HMIS.

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

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

Overview

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

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

What is Being Shared

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

Information shared to the participating agencies include:

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

How Your Information May Be Used

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

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

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

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

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

Your Rights Regarding Your Information in HMIS

- You have the right to opt-out of having yours and your household members' information shared to partnering agencies in the Northeast Illinois Homeless Management Information System (HMIS). To do so, you must request and sign the "Client Data Sharing Refusal Form." Any information in the HMIS prior to signing the Sharing Refusal form will continue to be shared with the agencies as described in this notice.

- You may request a list of current HMIS partner organizations from [Agency Name] or DuPage County Community Services, or review the current list at suburbancook.org/privacy. DuPage County Community Services may add new HMIS partner organizations to this list at any time.

- You have the right to inspect and obtain a copy of your own protected personal information for as long as it is kept in the HMIS, except for information compiled in reasonable anticipation of, or for use in, a legal proceeding.

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

Enforcement of Your Rights

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

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

[Agency Contact Information]	DuPage County Community Services
[Address]	HMIS System Administrator
[Address]	421 N County Farm Road
[Phone Number]	Wheaton, IL 60187
[Website]	630-407-6397
	dupageco.org/HMIS

Change History

- October 2009- Initial Policy was a part of client consent documents

- October 2012 - Adopted HUD's baseline privacy notice and detailed our implied consent disclosure process

- October 2014 – Updated HUD's baseline privacy notice to include Suburban Cook County, address the name change of DuPage County HMIS to Northeast Illinois HMIS, and reflect the changes to the list of shared data elements.

- xx 2020 – Complete reorganization, re-formatting, deduplication of statements, and adjusted level of language used. Added language around sharing of pre-existing data after a client

refuses to share any new information. Moved to using Effective data rather than version numbers.

to adopt to enhance further the privacy and security of information collected through HMIS. Organizations are encouraged to apply these additional protections to protect client information as they deem appropriate. They must also comply with federal, state and local laws that require additional confidentiality protections.

This two-tiered approach recognizes the broad diversity of organizations that participate in HMIS and the differing programmatic and organizational realities that may demand a higher standard for some activities. Some organizations (*e.g.*, such as those serving victims of domestic violence) may choose to implement higher levels of privacy and security standards because of the nature of their homeless population and/or service provision. Others (*e.g.*, large emergency shelters) may find the higher standards overly burdensome or impractical. At a minimum, however, all organizations must meet the baseline privacy and security requirements described in this section. This approach provides a uniform floor of protection for homeless clients with the possibility of additional protections for organizations with additional needs or capacities.

Sections 4.1 and 4.2 discuss HMIS privacy standards. Section 4.3 discusses security standards.

4.1. HMIS Privacy Standards: Definitions and Scope

4.1.1. Definition of Terms

1. *Protected Personal Information (PPI).* Any information maintained by or for a Covered Homeless Organization about a living homeless client or homeless individual that: (1) Identifies, either directly or indirectly, a specific individual; (2) can be manipulated by a reasonably foreseeable method to identify a specific individual; or (3) can be linked with other available information to identify a specific individual.

2. *Covered Homeless Organization (CHO).* Any organization (including its employees, volunteers, affiliates, contractors, and associates) that records, uses or processes PPI on homeless clients for an HMIS.

3. *Processing.* Any operation or set of operations performed on PPI, whether or not by automated means, including but not limited to collection, maintenance, use, disclosure, transmission and destruction of the information.

4. *HMIS Uses and Disclosures.* The uses and disclosures of PPI that are allowed by these standards.

4.1.2. Applying the HMIS Privacy and Security Standards

These privacy standards apply to any homeless assistance organization that records, uses or processes protected personal information (PPI) for an HMIS. A provider that meets this definition is referred to as a covered homeless organization (CHO). All PPI maintained by a CHO is subject to these standards.

Any CHO that is covered under the HIPAA is not required to comply with the privacy or security standards in this Notice if the CHO determines that a substantial portion of its PPI about homeless clients or homeless individuals is protected health information as defined in the HIPAA rules. Exempting HIPAA covered entities from the HMIS privacy and security rules avoids all possible conflicts between the two sets of rules. The HMIS standards give precedence to the HIPAA privacy and security rules because: (1) The HIPAA rules are more finely attuned to the requirements of the health care system; (2) the HIPAA rules provide important privacy and security protections for protected health information; and (3) requiring a homeless provider to comply with or reconcile two sets of rules would be an unreasonable burden.

It is possible that part of a homeless organization's operations may be covered by the HMIS standards while another part is covered by the HIPAA standards. A CHO that, because of organizational structure, legal requirement, or other reason, maintains personal information about a homeless client that does not fall under the privacy and security standards in this section (*e.g.*, the information is subject to the HIPAA health privacy rule) must describe that information in its privacy notice and explain the reason the information is not covered. The purpose of the disclosure requirement is to avoid giving the impression that all personal information will be protected under the HMIS standards if other standards or if no standards apply.

4.1.3. Allowable HMIS Uses and Disclosures of Protected Personal Information (PPI)

A CHO may use or disclose PPI from an HMIS under the following circumstances: (1) To provide or coordinate services to an individual; (2) for functions related to payment or reimbursement for services; (3) to carry out administrative functions, including but not limited to legal, audit, personnel, oversight and management functions; or (4) for creating de-identified PPI.

CHOs, like other institutions that maintain personal information about individuals, have obligations that may transcend the privacy interests of clients. The following additional uses and disclosures recognize those obligations to use or share personal information by balancing competing interests in a responsible and limited way. Under the HMIS privacy standard, these additional uses and disclosures are permissive and not mandatory (except for first party access to information and any required disclosures for oversight of compliance with HMIS privacy and security standards). However, nothing in this standard modifies an obligation under applicable law to use or disclose personal information.

Uses and disclosures required by law. A CHO may use or disclose PPI when required by law to the extent that the use or disclosure complies with and is limited to the requirements of the law.

Uses and disclosures to avert a serious threat to health or safety. A CHO may, consistent with applicable law and standards of ethical conduct, use or disclose PPI if: (1) The CHO, in good faith, believes 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.

Uses and disclosures about victims of abuse, neglect or domestic violence. A CHO may disclose PPI about an individual whom the CHO reasonably believes to be a victim of abuse, neglect or domestic violence to a government authority (including a social service or protective services agency) authorized by law to receive reports of abuse, neglect or domestic violence under any of the following circumstances:

- Where the disclosure is required by law and the disclosure complies with and is limited to the requirements of the law;
- If the individual agrees to the disclosure; or
- To the extent that the disclosure is expressly authorized by statute or regulation; and the CHO believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or 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.

A CHO that makes a permitted disclosure about victims of abuse, neglect or domestic violence must promptly inform the individual that a disclosure has been or will be made, except if:

- The CHO, in the exercise of professional judgment, believes informing the individual would place the individual at risk of serious harm; or
- The CHO would be informing a personal representative (such as a family member or friend), and the CHO reasonably believes 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 determined by the CHO, in the exercise of professional judgment.

Uses and disclosures for academic research purposes. A CHO may use or disclose PPI for academic research conducted by an individual or institution that has a formal relationship with the CHO if the research is conducted either:

- 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 program administrator (other than the individual conducting the research) designated by the CHO; or
- By an institution for use in a research project conducted under a written research agreement approved in writing by a program administrator designated by the CHO.

A written research agreement must: (1) Establish rules and limitations for the processing and security of PPI in the course of the research; (2) provide for the return or proper disposal of all PPI at the conclusion of the research; (3) restrict additional use or disclosure of PPI, except where required by law; and (4) require that the recipient of data formally agree to comply with all terms and conditions of the agreement.

A written research agreement is not a substitute for approval of a research project by an Institutional Review Board, Privacy Board or other applicable human subjects protection institution.

Disclosures for law enforcement purposes. A CHO may, consistent with applicable law and standards of ethical conduct, disclose PPI for a law enforcement purpose to a law enforcement official under any of the following circumstances:

- In response to a lawful court order, court-ordered warrant, subpoena or summons issued by a judicial officer, or a grand jury subpoena;
- If the law enforcement official makes a written request for protected personal information that: (1) Is signed by a supervisory official of the law enforcement agency seeking the PPI; (2) states that the information is relevant and material to a legitimate law enforcement investigation; (3) identifies the PPI sought; (4) is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought; and (5) states that de-identified information could not be used to accomplish the purpose of the disclosure.
- If the CHO believes in good faith that the PPI constitutes evidence of criminal conduct that occurred on the premises of the CHO;
- 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
- If (1) 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 (2) 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.

4.2. Privacy Requirements

All CHOs must comply with the baseline privacy requirements described here with respect to: data collection limitations; data quality; purpose and use limitations; openness; access and correction; and accountability. A CHO may adopt additional substantive and procedural privacy protections that exceed the baseline requirements for each of these areas. A CHO must comply with federal, state and local laws that require additional confidentiality protections. All additional protections must be described in the CHO's privacy notice. A CHO must comply with all baseline privacy protections and with all additional privacy protections included in its privacy notice.

A CHO may maintain a common data storage medium with another organization (including but not limited to another CHO) that includes the sharing of PPI. When PPI is shared between organizations, responsibilities for privacy and security may reasonably be allocated between the organizations. Organizations sharing a common data storage medium and PPI may adopt differing privacy and security policies as they deem appropriate, administratively feasible, and consistent with these HMIS privacy and security standards, as long as these privacy and security policies allow for the unduplication of homeless clients at the CoC level.

4.2.1. Collection Limitation

Baseline requirement. A CHO may collect PPI only when appropriate to the purposes for which the information is obtained or when required by law. A CHO must collect PPI by lawful and fair means and, where appropriate, with the knowledge or consent of the individual.

A CHO must post a sign at each intake desk (or comparable location) that explains generally the reasons for collecting this information. Consent of the individual for data collection may be inferred from the circumstances of the collection. Providers may use the following language to meet this standard: ''We collect personal information directly from you for reasons that are discussed in our privacy statement. 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 for homeless persons, and to better understand the needs of homeless persons. We only collect information that we consider to be appropriate.''

Additional Privacy Protections. A CHO may, in its privacy notice, commit itself to additional privacy protections consistent with HMIS requirements, including, but not limited to:

(1) Restricting collection of personal data, other than required HMIS data elements;

(2) Collecting PPI only with the express knowledge or consent of the individual (unless required by law); and

(3) Obtaining oral or written consent from the individual for the collection of personal information from the individual or from a third party.

4.2.2. Data Quality

Baseline Requirement. PPI collected by a CHO must be relevant to the purpose for which it is to be used. To the extent necessary for those purposes, PPI should be accurate, complete and timely.

A CHO must develop and implement a plan to dispose of or, in the alternative, to remove identifiers from, PPI that is not in current use seven years after the PPI was created or last changed

(unless a statutory, regulatory, contractual, or other requirement mandates longer retention). Standards for destroying information are provided in Section 4.3.

4.2.3. Purpose Specification and Use Limitation

Baseline Requirement. A CHO must specify in its privacy notice the purposes for which it collects PPI and must describe all uses and disclosures. A CHO may use or disclose PPI only if the use or disclosure is allowed by this standard and is described in its privacy notice. A CHO may infer consent for all uses and disclosures specified in the notice and for uses and disclosures determined by the CHO to be compatible with those specified in the notice.

Except for first party access to information and any required disclosures for oversight of compliance with HMIS privacy and security standards, all uses and disclosures are permissive and not mandatory. Uses and disclosures not specified in the privacy notice can be made only with the consent of the individual or when required by law.

Additional Privacy Protections. A CHO may, in its privacy notice, commit itself to additional privacy protections consistent with HMIS requirements, including, but not limited to:

(1) Seeking either oral or written consent for some or all processing when individual consent for a use, disclosure or other form of processing is appropriate;

(2) Agreeing to additional restrictions on use or disclosure of an individual's PPI at the request of the individual if the request is reasonable. The CHO is bound by the agreement, except if inconsistent with legal requirements;

(3) Limiting uses and disclosures to those specified in its privacy notice and to other uses and disclosures that are necessary for those specified;

(4) Committing that PPI may not be disclosed directly or indirectly to any government agency (including a contractor or grantee of an agency) for inclusion in any national homeless database that contains personal protected information unless required by statute;

(5) Committing to maintain an audit trail containing the date, purpose and recipient of some or all disclosures of PPI;

(6) Committing to make audit trails of disclosures available to the homeless individual; and

(7) Limiting disclosures of PPI to the minimum necessary to accomplish the purpose of the disclosure.

4.2.4. Openness

Baseline Requirement. A CHO must publish a privacy notice describing its polices and practices for the processing of PPI and must provide a copy of its privacy notice to any individual upon request. If a CHO maintains a public web page, the CHO must post the current version of its privacy notice on the web page. A CHO may, if appropriate, omit its street address from its privacy notice. A CHO must post a sign stating the availability of its privacy notice to any individual who requests a copy.

A CHO must state in its privacy notice that the policy may be amended at any time and that amendments may affect information obtained by the CHO before the date of the change. An amendment to the privacy notice regarding use or disclosure will be effective with respect to information processed before the amendment, unless otherwise stated. All amendments to the privacy notice must be consistent with the requirements of these privacy standards. A CHO must maintain permanent documentation of all privacy notice amendments.

CHOs are reminded that they are obligated to provide reasonable accommodations for persons with disabilities throughout the data collection process. This may include but is not limited to, providing qualified sign language interpreters, readers or materials in accessible formats such as Braille, audio, or large type, as needed by the individual with a disability. *See* 24 CFR 8.6; 28 CFR 36.303. **Note:** This obligation does not apply to CHOs who do not receive federal financial assistance and who are also exempt from the requirements of Title III of the Americans with Disabilities Act because they qualify as ''religious entities'' under that Act.

In addition, CHOs that are recipients of federal financial assistance shall provide required information in languages other than English that are common in the community, if speakers of these languages are found in significant numbers and come into frequent contact with the program. *See HUD Limited English Proficiency Recipient Guidance* published on December 18, 2003 (68 FR 70968).

Additional Privacy Protections. A CHO may, in its privacy notice, commit itself to additional privacy protections consistent with HMIS requirements, including, but not limited to:

(1) making a reasonable effort to offer a copy of the privacy notice to each client at or around the time of data collection or at another appropriate time;

(2) giving a copy of its privacy notice to each client on or about the time of first data collection. If the first contact is over the telephone, the privacy notice may be provided at the first in-person contact (or by mail, if requested); and/or

(3) adopting a policy for changing its privacy notice that includes advance notice of the change, consideration of public comments, and prospective application of changes.

4.2.5. Access and Correction

Baseline Requirement. In general, a CHO must allow an individual to inspect and to have a copy of any PPI about the individual. A CHO must offer to explain any information that the individual may not understand.

A CHO must consider any request by an individual for correction of inaccurate or incomplete PPI pertaining to the individual. A CHO is not required to remove any information but may, in the alternative, mark information as inaccurate or incomplete and may supplement it with additional information.

In its privacy notice, a CHO may reserve the ability to rely on the following reasons for denying an individual inspection or copying of the individual's PPI:

(1) Information compiled in reasonable anticipation of litigation or comparable proceedings;

(2) information about another individual (other than a health care or homeless provider);

(3) information obtained under a promise of confidentiality (other than a promise from a health care or homeless provider) if disclosure would reveal the source of the information; or

(4) information, the disclosure of which would be reasonably likely to endanger the life or physical safety of any individual.

A CHO can reject repeated or harassing requests for access or correction. A CHO that denies an individual's request for access or correction must explain the reason for the denial to the individual and must include documentation of the request and the reason for the denial as part of the protected personal information about the individual.

Additional Privacy Protections. A CHO may, in its privacy notice, commit itself to additional privacy protections consistent with HMIS requirements, including, but not limited to:

(1) Accepting an appeal of a denial of access or correction by adopting its own

appeal procedure and describing the procedure in its privacy notice;

(2) Limiting the grounds for denial of access by not stating a recognized basis for denial in its privacy notice;

(3) Allowing an individual whose request for correction has been denied to add to the individual's information a concise statement of disagreement. A CHO may agree to disclose the statement of disagreement whenever it discloses the disputed PPI to another person. These procedures must be described in the CHO's privacy notice; and/or

(4) Providing to an individual a written explanation of the reason for a denial of an individual's request for access or correction.

4.2.6. Accountability

Baseline Requirement. A CHO must establish a procedure for accepting and considering questions or complaints about its privacy and security policies and practices. A CHO must require each member of its staff (including employees, volunteers, affiliates, contractors and associates) to sign (annually or otherwise) a confidentiality agreement that acknowledges receipt of a copy of the privacy notice and that pledges to comply with the privacy notice.

Additional Privacy Protections. A CHO may, in its privacy notice, commit itself to additional privacy protections consistent with HMIS requirements, including, but not limited to:

(1) Requiring each member of its staff (including employees, volunteers, affiliates, contractors and associates) to undergo (annually or otherwise) formal training in privacy requirements;

(2) Establishing a method, such as an internal audit, for regularly reviewing compliance with its privacy policy;

(3) Establishing an internal or external appeal process for hearing an appeal of a privacy complaint or an appeal of a denial of access or correction rights; and/or

(4) Designating a chief privacy officer to supervise implementation of the CHO's privacy standards.

4.3. Security Standards

This section describes the standards for system, application and hard copy security. All CHOs must comply with the baseline security requirements. A CHO may adopt additional security protections that exceed the baseline requirements if it chooses.

4.3.1. System Security

Applicability. Baseline Requirement. A CHO must apply system security provisions to all the systems where personal protected information is stored, including, but not limited to, a CHO's networks, desktops, laptops, mini-computers, mainframes and servers.

Additional Security Protections. A CHO may commit itself to additional security protections consistent with HMIS requirements by applying system security provisions to all electronic and hard copy information that is not collected specifically for the HMIS. A CHO may also seek an outside organization to perform an internal security audit and certify system security.

User Authentication. Baseline Requirement. A CHO must secure HMIS systems with, at a minimum, a user authentication system consisting of a username and a password. Passwords must be at least eight characters long and meet reasonable industry standard requirements. These requirements include, but are not limited to:

(1) Using at least one number and one letter;

(2) Not using, or including, the username, the HMIS name, or the HMIS vendor's name; and/or

(3) Not consisting entirely of any word found in the common dictionary or any of the above spelled backwards.

Using default passwords on initial entry into the HMIS application is allowed so long as the application requires that the default password be changed on first use. Written information specifically pertaining to user access (*e.g.*, username and password) may not be stored or displayed in any publicly accessible location. Individual users must not be able to log on to more than one workstation at a time, or be able to log on to the network at more than one location at a time.

Additional Security Protections. A CHO may commit to additional security protections consistent with HMIS requirements by including one of each of the following kinds of characters in the password:

(1) upper and lower-case letters;

(2) numbers; and/or

(3) symbols.

A common solution to creating complex passwords is to use phrases instead of individual words as passwords, capitalize each new word in the phrase, and substitute numbers and symbols for letters in any given word. For example, the phrase ''secure password'' can be modified to ''$3cur3P@$$w0rd'' by replacing the letter ''s'' with ''$,'' the letter ''e'' with the number ''3,'' the letter ''a'' with ''@'' and the letter ''o'' with the number ''0,'' and eliminating spaces between words.

Virus Protection. Baseline Requirement. A CHO must protect HMIS systems from viruses by using commercially available virus protection software. Virus protection must include automated scanning of files as they are accessed by users on the system where the HMIS application is housed. A CHO must regularly update virus definitions from the software vendor.

Additional Security Protections. A CHO may commit itself to additional security protections consistent with HMIS requirements by automatically scanning all files for viruses when the system is turned on, shut down or not actively being used.

Firewalls. Baseline Requirement. A CHO must protect HMIS systems from malicious intrusion behind a secure firewall. Each individual workstation does not need its own firewall, as long as there is a firewall between that workstation and any systems, including the Internet and other computer networks, located outside of the organization. For example, a workstation that accesses the Internet through a modem would need its own firewall. A workstation 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. Older operating systems can be equipped with secure firewalls that are available both commercially and for free on the Internet.

Additional Security Protections. A CHO may commit itself to additional security protections consistent with HMIS requirements by applying a firewall to all HMIS workstations and systems.

Public Access. Baseline Requirement. HMIS that use public forums for data collection or reporting must be secured to allow only connections from previously approved computers and systems through Public Key Infrastructure (PKI) certificates, or extranets that limit access based on the Internet Provider (IP) address, or similar means. A public forum includes systems with public access to any part of the computer through the Internet, modems, bulletin boards, public kiosks or similar arenas. Further information on these tools can be found in the HMIS Consumer Guide and the HMIS Implementation Guide, both available on HUD's Web site.

Additional Security Protections. A CHO may commit itself to additional security protections consistent with HMIS requirements by using PKI certificates and extranets that limit access based on the IP address. A very secure system would not house any

HMIS data on systems that are accessible to the general public.

Physical Access to Systems With Access to HMIS Data. Baseline Requirement. A CHO must staff computers stationed in public areas that are used to collect and store HMIS data at all times. When workstations are not in use and staff are not present, steps should be taken to ensure that the computers and data are secure and not usable by unauthorized individuals. After a short amount of time, workstations should automatically turn on a password protected screen saver when the workstation is temporarily not in use. Password protected screen savers are a standard feature with most operating systems and the amount of time can be regulated by a CHO. If staff from a CHO will be gone for an extended period of time, staff should log off the data entry system and shut down the computer.

Additional Security Protections. A CHO may commit itself to additional security protections consistent with HMIS requirements by automatically logging users off of the HMIS application after a period of inactivity and automatically logging users off of the system after a period of inactivity. Most server operating systems come equipped with the needed software to automatically perform these functions. If staff from a CHO will be gone for an extended period of time, staff should store the computer and data in a locked room.

Disaster Protection and Recovery. Baseline Requirement. A CHO must copy all HMIS data on a regular basis to another medium (*e.g.*, tape) and store it in a secure off-site location where the required privacy and security standards would also apply. A CHO that stores data in a central server, mini-computer or mainframe must store the central server, mini-computer or mainframe in a secure room with appropriate temperature control and fire suppression systems. Surge suppressors must be used to protect systems used for collecting and storing all the HMIS data.

Additional Security Protections. A CHO may commit itself to additional security protections consistent with HMIS requirements by providing, among other options, fire and water protection at the off-site location that houses the storage medium. A CHO may also seek an outside organization to conduct a disaster protection audit.

Disposal. Baseline Requirement. In order to delete all HMIS data from a data storage medium, a covered homeless organization must reformat the storage medium. A CHO should reformat the storage medium more than once before reusing or disposing the medium.

Additional Security Protections. A CHO may commit itself to additional security protections consistent with HMIS requirements by destroying media at a bonded vendor to ensure all the HMIS data is completely destroyed.

System Monitoring. Baseline Requirement. A CHO must use appropriate methods to monitor security systems. Systems that have access to any HMIS data must maintain a user access log. Many new operating systems and web servers are equipped with access logs and some allow the computer to email the log information to a designated user, usually a system administrator. Logs must be checked routinely.

Additional Security Protections. A CHO may commit itself to additional security protections consistent with HMIS requirements by checking user access logs routinely for inappropriate access, hardware and software problems, errors and viruses, or purchasing one of several software applications available that track the status of individual files on computers. These applications are used to make sure that files are not being changed when they are not supposed to be. The applications inform the system administrator if a computer has been hacked, infected with a virus, has been restarted, or if the data files have been tampered with.

4.3.2. Application Security

These provisions apply to how all the HMIS data are secured by the HMIS application software.

Applicability. Baseline Requirement. A CHO must apply application security provisions to the software during data entry, storage and review or any other processing function.

Additional Security Protections. A CHO may commit itself to additional security protections consistent with HMIS requirements as needed.

User Authentication. Baseline Requirement. A CHO must secure all electronic HMIS data with, at a minimum, a user authentication system consisting of a username and a password. Passwords must be at least eight characters long and meet reasonable industry standard requirements. These requirements include, but are not limited to:

(1) Using at least one number and one letter;

(2) Using default passwords on initial entry into the HMIS application is allowed so long as the application requires that the default password be changed on first use;

(3) Not using, or including, the username, the HMIS name, or the HMIS vendor's name; and

(4) Not consisting entirely of any word found in the common dictionary or any of the above spelled backwards.

Written information specifically pertaining to user access (*e.g.*, username and password) may not be stored or displayed in any publicly accessible location. Individual users should not be able to log on to more than one workstation at a time, or be able to log on to the network at more than one location at a time.

Additional Security Protections. A CHO may commit itself to additional security protections consistent with HMIS requirements by including one of each of the following kinds of characters in the password:

(1) Upper and lower-case letters;

(2) Numbers; and

(3) Symbols.

A common solution to creating complex passwords is to use phrases instead of individual words as passwords, capitalize each new word in the phrase and substitute numbers and symbols for letters in any given word. For example, the phrase ''secure password'' can be modified to ''$3cur3P@$$w0rd'' by replacing the letter ''s'' with ''$,'' the letter ''e'' with the number ''3,'' the letter ''a'' with ''@'' and the letter ''o'' with the number ''0,'' and eliminating spaces between words.

Electronic Data Transmission. Baseline Requirement. A CHO must encrypt all HMIS data that are electronically transmitted over the Internet, publicly accessible networks or phone lines to current industry standards. The current standard is 128-bit encryption. Unencrypted data may be transmitted over secure direct connections between two systems. A secure direct connection is one that can only be accessed by users who have been authenticated on at least one of the systems involved and does not utilize any tertiary systems to transmit the data. A secure network would have secure direct connections.

Additional Security Protections. A CHO may commit itself to additional security protections consistent with HMIS requirements by using PKI certificates to verify the workstations involved in the electronic data transmission, and by restricting access between the workstations using IP addresses. A very secure system would not transmit any protected information over a public system like the Internet.

Electronic Data Storage. Baseline Requirement. A CHO must store all HMIS data in a binary, not text, format. A CHO that uses one of several common

applications (*e.g.*, Microsoft Access, Microsoft SQL Server and Oracle) are already storing data in binary format and no other steps need to be taken.

Additional Security Protections. A CHO may commit itself to additional security protections consistent with HMIS requirements by requiring that all PPI be stored in an encrypted format using at least the current industry standard. The current standard is a 128-bit key.

4.3.3. Hard Copy Security

This section provides standards for securing hard copy data.

Applicability. Baseline Requirement. A CHO must secure any paper or other hard copy containing personal protected information that is either generated by or for HMIS, including, but not limited to reports, data entry forms and signed consent forms.

Additional Security Protections. A CHO may commit itself to additional security protections consistent with HMIS requirements by applying hard copy security provisions to paper and hard copy information that is not collected specifically for the HMIS.

Security. Baseline Requirement. A CHO must supervise at all times any paper or other hard copy generated by or for HMIS that contains PPI when the hard copy is in a public area. When CHO staff are not present, the information must be secured in areas that are not publicly accessible.

Written information specifically pertaining to user access (*e.g.*, username and password) must not be stored or displayed in any publicly accessible location.

5. Technical Standards

This section presents the technical standards that will be required for HMIS applications and for the organizations responsible for storing HMIS data. Except as otherwise provided, these standards do not specify or recommend any particular operating system, development environment, networking environment, database, hardware or other aspect of the HMIS application. This part of the Notice is primarily directed to HMIS developers and CoC system administrators.

5.1. Required HMIS Capabilities

5.1.1. Automatic Generation of Identification Numbers and Information

Based on the data collected through the client assessment process, program staff interviews, self-administered forms or review of case management records, the HMIS application must be capable of automatically generating data for each record. This capability includes the automatic generation of:

(1) Unique *Personal Identification Numbers (PINs)* for persons who have not been previously served within the CoC, and reassignment of PINs for persons who have been served previously within a program and/or the CoC;

(2) *Program Identification Information* that is uniquely associated with each program within a CoC and is assigned to every service episode for each client; and,

(3) *Household Identification Numbers* for persons who have been identified as members of a household that participated in the same service episode.

Personal Identification Numbers (PINs). A PIN is a number automatically generated by the HMIS application. All records associated with the same person should be assigned the same PIN. There is no required format for the PIN as long as there is a single unique PIN for every client served in the CoC and it contains no personally-identifying information. The PIN is used to produce an unduplicated count of all persons at three levels: (1) Within a single program; (2) across multiple programs that share HMIS data (where programs agree to share such data); and/or (3) across the entire CoC database, whether or not data are shared across programs within a CoC. At each level, an HMIS must be capable of searching client records to determine if clients have been previously served. The search must involve the matching of client records using personal identifier fields (*e.g.*, Name, Social Security Number, Date of Birth, and Gender) to retrieve a record(s) with identical or similar values in each of these fields.

Program Identification Information. Program identification information for every program offered in a CoC consists of the following four fields:

(1) Federal Information Processing Standards (FIPS) Code. To find the 10-digit FIPS code consisting of a 2-digit state code, 3-digit county code and 5-digit place code: (1) Go to Web site *http://geonames.usgs.gov/fips55.html;* (2) click on ''Search the FIPS55 Data Base;'' (3) click on state from ''State Number Code'' pull down menu (this also tells you 2-digit state code); (4) type town or city name in ''FIPS 55 Feature Name'' box; and (5) click on ''Send Query'' and 3-digit county code and 5-digit place code will be shown;

(2) Facility Code (to be locally determined);

(3) Continuum of Care (CoC) Code (HUD-assigned); and

(4) Program Type Code:

1 = Emergency shelter (*e.g.*, facility or vouchers)

2 = Transitional housing

3 = Permanent supportive housing

4 = Street outreach

5 = Homeless prevention (*e.g.*, security deposit or one month's rent)

6 = Services-only type of program

7 = Other

The FIPS code, facility code, CoC code and program type code should be separate fields in the HMIS application. There is no requirement to merge them into a single field. For each client intake program staff are only required to enter the program type code. Programs may choose to provide more detailed response categories for the services-only type program response. However, for reporting purposes, these detailed categories must be collapsed into a single service-only type category and its associated code.

A corresponding FIPS code, facility code and CoC code should be automatically generated by the HMIS based on which facility is doing the intake. Once program identification information has been created, the HMIS must ensure that the information is associated with every service episode recorded within the CoC.

Household Identification Numbers. HMIS must generate the same Household Identification Number for every person designated by program staff as being together for an episode of service. The household identification numbers assigned will be maintained in each person's permanent record and will be unique for each service episode experienced by the client.

As discussed in previous parts of this final Notice, when a group of persons apply for services together (as a household or family), information is first recorded for the household head who is applying for services and then information is recorded for any children under 18 years of age who are applying for services with the household head. The children do not need to be present at the time the household head applies for services. The same household identification number is assigned to the adult head of household and any children who have been identified as applying for services with the head. If there are other adult members of the household (over 18 years of age) who are reported to be part of this household, a separate intake is conducted. As part of this intake, this individual is assigned the same household identification number as the other household members.

5.1.2. Missing Value Categories

A limited number of data elements require ''don't know,'' ''not applicable'' and ''refused'' response categories for close-ended questions. These missing value categories and their associated codes should appear on the same list as the valid responses. For open-ended questions (*e.g.*, name), the HMIS application should include the ''don't know,'' ''not applicable'' and ''refused'' response categories for each field in the data element (*e.g.*, first name, last name, middle initial and suffix).

5.1.3. Other Response Categories

Certain data elements may contain a response category labeled ''other.'' When a data element contains such an option, there should also be within the same database table a separate alphanumeric field where the ''other'' value may be entered by program staff. For instance, a coded field that accepts the values ''0=Red,'' ''1=Yellow,'' or ''9=Other'' should have an accompanying field that accepts open-ended answers such as tangerine, blue or magenta.

5.1.4. Response Category Codes

Where character or numeric codes are shown next to each response category, only the character or numeric response code needs to be stored in the database. For example, ''1=Yes'' will be the response code on the computer screen or hard copy, but the electronic database can store ''1=Yes'' responses as ''1'' in the database. For open-ended or text answers (such as name), the full text answer or an encrypted version of it should be stored in the database.

5.1.5. Exit Dates

The HMIS should identify programs that have fixed lengths of enrollment. When a client enters such a program, the HMIS should automatically generate the exit date based on the entry date and the program's fixed length of enrollment. For example, an overnight emergency shelter has a fixed length of stay of one day. This information would be stored with the other program information like FIPS code and program code. When a client enrolls in an overnight emergency shelter, the HMIS will automatically set the client's exit date for the next day.

5.1.6. Maintaining Historical Data

An HMIS should have the ability to record client data from a limitless number of service transactions for longitudinal data analysis and assessment of client outcomes (often referred to as a ''transactional'' or ''relational'' database structure). A transactional or relational database organizes data within a set of tables from which data can be accessed or reassembled in many different ways without having to erase historical data or reorganize the database tables. For example, an HMIS may include a table that describes a client's demographic profile with columns for name, SSN, date of birth, gender, and so on. In most cases, the information in the profile table will not change. Another table may describe the client's income status: source of income, amount of income from each source, receipt of non-cash benefits, and so forth. The information in the income status table may change overtime, but all historical data should be preserved. Additional tables may include data from each service encounter by program type (*e.g.*, mental health and/or substance abuse).

5.1.7. Data Export

Although a standard environment is not specified, any HMIS application must be capable of exporting any and all data collected into a comma-separated values text file using the following format:

- All fields in a given record are separated by a comma;
- All records within a given text file contain the same fields;
- Blank fields are signified by the comma ending the previous field (or the beginning of the line if the field is the first in the record) followed by a comma indicating the end of the empty field;
- Fields containing text information (as opposed to numeric) will be surrounded by double quotes whenever the field includes blank spaces, commas, or other symbols not part of the standard alphabet;
- The first line of the file shall be a list of the field names included in every record in the file; and
- The list of field names shall be in the same format described above.

5.2. Continuum of Care Requirements

5.2.1. Storage Requirements

The CoC must have or designate a central coordinating body that will be responsible for centralized collection and storage of HMIS data.

HMIS data must be collected to a central location at least once a year from all HMIS users within the CoC.

HMIS data must be stored at the central location for a minimum of seven years after the date of collection by the central coordinating body or designee of the CoC. The seven-year requirement is the current government standard for health and medical information.

Environmental Impact

This notice does not direct, provide for assistance or loan and mortgage insurance for, or otherwise govern or regulate, real property acquisition, disposition, leasing, rehabilitation, alteration, demolition, or new construction, or establish, revise or provide for standards for construction or construction materials, manufactured housing, or occupancy. Accordingly, under 24 CFR 50.19(c)(1), this notice is categorically excluded from environmental review under the National Environmental Policy Act of 1969 (42 U.S.C. 4321).

Dated: July 21, 2004.

Nelson R. Bregón,

General Deputy Assistant Secretary for Community Planning and Development.

[FR Doc. 04–17097 Filed 7–29–04; 8:45 am]

BILLING CODE 4210–29–P

Data & Performance
(formerly identified as HMIS Policy Committee)

Purpose:
The purpose of the Data and Performance Measurement Committee is to ensure local compliance with HUD Homelessness Management Information System (HMIS) data standards, improve agency and community-wide data quality, as well as use HMIS data and Coordinated Entry System data to inform Continuum of Care program/system design and measure progress on community goals and plans to end homelessness.
The Committee is responsible for gathering data and providing analysis of projects including homeless service and housing inventories, counts, and surveys (note: A = Homeless & Non-Homeless Providers B = Homeless Providers HEARTH Only)

CoC Strategy for Data & Performance Meas.	CY2021 Objectives
Strengthen **collection** of essential data sources	A) 100% of Homeless providers and non-homeless service providers contribute to shared data environment.
	B) The Continuum of Care meets the minimum Data Quality Standards.
	A) & B) Develop plan, which includes timeline and Homeless vs non-homeless service providers expectations, to strive for meeting Coordinated entry placement and referral needs.
	A) & B) Customized local data elements are limited to information needed to report, serve, and house clients.
Strengthen **reporting** of essential data sources	A) & B) System Performance Measures and Data Performance Reports are provided and reviewed by appropriate Committees at each meeting
	B) Publicly available static dashboard posted on Continuum Website on a quarterly basis
Strengthen **utilization** of essential data sources	A) Individual agencies are encouraged to know existing reports/charts prior to creating custom reports/charts utilizing their own data
	A) All homeless providers and non-homeless providers work together to remove systemic barriers to housing and services by utilizing data driven decisions
Promote [data collection] strategies to strengthen local efforts to identify people experiencing chronic homelessness and frequent users of shelter and other systems	A) & B) Utilize a relaxed client centered approach to obtaining minimum required data to engage in services

Commented [TJ1]: This is HMIS data, currently, however there is activity happening outside of HMIS that is being missed.

Commented [WM2]: Committee seeks to have a HUD vs Hearth split on the rate of contribution

Commented [TJ3]: This sounds like the data quality plan that exists but may need review/expansion to include locally adopted data elements, timeline for implementation, etc.

Commented [WM4]: Committee commented that we need a communications plan for this.

Commented [TJ5R4]: HMIS Staff are continuing to plan to be at as many committee tables as we can. Conflicts with HP and seeking to see if I can start being present at Leadership and Grants Funding. Hope to have more members of this and other committees become more familiar with the tools available.

Commented [TJ6]: Agencies won't all have report writing abilities unless they have someone dedicated to reporting who we can train. Otherwise, they will be able to drill down their data in Qlik Sense, use Canned Reports, or report writer for quick counts, or request HMIS to assist when appropriate.

Commented [TJ7]: I hear that the HP group is doing something pretty cool – streamlined referral and application process for the DuPage County CRF funding. Reached out to Amy to see how HMIS can help.

Commented [WM8]: We determined we will need to set benchmarks for the objectives as weel as any educaton/communcation plans to active objectives

Commented [TJ9R8]: Consider starting with existing data quality measures such as the 0640 (source) data points (to be identified – specifically those that may be more problematic)

Commented [TJ10R8]: Also, reference the Data Quality plan for this.